Bedienungsanleitung,

Konfigurationsanleitung

und

technische Spezifikation

für die

VPN Appliance

der

msm net meissner GmbH

Version dieser Dokumentation:
Release: 1.02
Datum: 09.03.2012

Irrtümer und technische Änderungen vorbehalten

Copyright© 2011 msm net meissner GmbH. Alle Rechte vorbehalten.

msm net wird in diesem Handbuch als Synomym für das msm net ingenieurbüro meissner und die msm net meissner GmbH verwendet.

Alle anderen in diesem Dokument genannten Warenzeichen dienen lediglich zu Identifikationszwecken. Sämtliche Handels-, Marken- und Warenzeichen sind Eigentum der jeweiligen Inhaber.
Die msm net meissner GmbH verzichtet auf alle Besitzrechte an Warenzeichen und Handelsbezeichnungen, die nicht ihr Eigentum sind.

Inhaltsverzeichnis

1.Vorwort....5
2.Konformitätserklärung....6
3.Sicherheitshinweise....7
3.1.Symbol und Hinweiserklärung....7
3.2.Grundlegende Sicherheitshinweise und Haftungsausschluß....8
4.Beschreibung des Gerätes....9
4.1.Bedienelemente der VPN Appliance....9
4.2.Anschlüsse auf der Rückseite der VPN Appliance....10
4.3.Funktionsbeschreibung....11
4.4.So erhalten Sie Unterstützung....12
5.Einbauanleitung....13
5.1.Vorbereitung am Aufstellort....13
5.2. Auspacken....14
5.2.Montage und Anschließen der VPN Appliance....15
5.3.Erstinbetriebnahme....16
6.Bedienung....19
6.1.Allgemeine Einstellungen....20
6.2.Datum und Uhrzeit....21
6.3.Benutzer Administration....22
6.4.Netzwerkschnittstellen....26
6.4.1.Internes Interface (LAN)....27
6.4.2.Externes Interface (WAN)....28
6.5.VPN Einstellungen....29
6.5.1.PKI Administration....30
6.5.2.IPSEC Administration....45
6.5.3.L2TP Administration....52
6.5.4.PPTP Administration....54
6.6.Firewall Einstellungen....56
6.7.Das Service Menü....61
6.7.1.Zuweisen eines Zertifikates für das Webinterface....62
6.7.2.RADIUS-Client....63
6.7.3.Routing Protokoll Konfiguration....64
6.7.4.Ipv6 Router Veröffentlichungsdienst....65
6.7.5.Systeminformationen....66
6.7.6.Netzwerk-Werkzeuge....67
6.8.Standortdaten....71
6.9.Logdatei....72
6.10.Upload und Download....73
7.Service und Wartung....74
8.Technische Daten....75
8.1.Bauformen....75
8.2.Leistungsparameter der VPN Appliance....76
8.3.Basis RFC der VPN Software....78
9.Entsorgungshinweise....79

1. Vorwort

Herzlichen Glückwunsch zu Ihrer Entscheidung, VPN Appliances von msm net für die Realisierung Ihrer VPN Lösungen einzusetzen.

Unsere Produkte basieren in allen Austattungsformen auf Standard IPC Komponenten und erfüllen alle unter dem Punkt 8.3 aufgelisteten internationalen Standards. Von diesen Fakten ausgehend ergibt sich für Sie eine sehr hohe Investitionssicherheit.

Für die Planung und Realisierung eines VPN müssen alle technischen belange von bestehenden Netzwerken sowie deren technische Anbindung an das Internet und die mobile Kommunikation des Außendienstes berücksichtigt werden.

Aus diesem Grund ist es von besonderer Bedeutung, dass zuerst eine IST-Analyse über alle zu integrierenden Bestandteile vorgenommen wird. Von dieser IST-Analyse ausgehend kann eine klare Zieldefinition mit allen umzusetzenden Maßnahmen und Anforderungen erfolgen.

Für die Realisierung ihrer VPN Lösung bieten wir Ihnen folgende Leistungen an:

- Beratungs-, Planungs- und Projektierungsleistungen zur Schaffung von VPN Lösungen im internationalen und nationalen Umfeld
- Erstellung eines Betriebskonzeptes für VPN - Netzwerke
- Erstellung eines Mengengerüstes für die Bestimmung der Hardwareanforderungen
- Installation, Konfiguration und Inbetriebnahme der Hard- und Software Ihrer Komponenten des VPN
- Überwachung und Auswertung von Protokolldateien
- regelmäßige Sicherheitsüberprüfungen
- Remote- und Vorort-Service und Wartung
- Einweisung und Schulung lokaler Administratoren

Durch die Nutzung unserer Produkte ist es möglich eine beliebige Anzahl von lokalen Netzwerken und Außendienstmitarbeitern in einem VPN über das Internet zu vernetzen.

Für weiterführende Informationen stehen wir Ihnen jederzeit gern zur Verfügung.

Dipl.- Ing. Manfred Meißner

msm net meissner GmbH

kompetent - kreativ - innovativ

EG – Konformitätserklärung

Hersteller:	msm net meissner GmbH
Anschrift:	Greizer Strasse 87 D – 07937 Zeulenroda-Triebes Bundesrepublik Deutschland
Produktbezeichnung:	Mini – VPN Appliance und Midi – VPN Appliance

Die bezeichneten Produkte stimmen in der von uns in Verkehr gebrachten Ausführung mit den Vorschriften folgender Europäischer Richtlinien überein:

2004/108/EG	Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten über die elektromagnetische Verträglichkeit
2006/95/EG	Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen

msm net meissner GmbH Zeulenroda, den 15.09.2010

Manfred Meißner Steffen Meißner

Diese Erklärung bescheinigt die Übereinstimmung mit den genannten Richtlinien, ist jedoch keine Zusicherung von Eigenschaften. Die Sicherheitshinweise der mitgelieferten Produktdokumentation sind zu beachten.
This declaration certifies the conformity to the specified directives but contains no assurance of proporties. The safety documentation accompanying the product shall be considered in detail.

3. Sicherheitshinweise

3.1. Symbol und Hinweiserklärung

Bitte beachten Sie die Bedeutung folgender Symbol- und Hinweiserklärungen. Sie repräsentieren unterschiedliche Gefahrenstufen.

VORSICHT	
	Bezeichnet eine mögliche gefährliche Situation. Wenn diese Informationen nicht befolgt werden, können Sachschäden sowie leichte oder mittlere Körperverletzungen die Folge sein.

HINWEIS	
	Bezeichnet allgemeine Informationen. Nützliche Anwender-Tipps und Arbeitsempfehlungen, welche aber keinen Einfluss auf die Sicherheit und Gesundheit von Personen haben.

3.2. Grundlegende Sicherheitshinweise und Haftungsausschluß

Diese Betriebsanleitung dient der bestimmungsgemäßen Verwendung der VPN Appliances von msm net. Insbesondere die Sicherheitshinweise sind von allen Personen zu beachten, die die Geräte installieren oder betreiben. Darüber hinaus sind die für den Einsatzort jeweils geltenden Regeln und Vorschriften zu beachten.

Eine unsachgemäße Ausführung der Installation oder der Konfiguration kann zu Schäden führen. Daher übernehmen wir keinerlei Verantwortung und Haftung für Verluste, Schäden oder Kosten, die sich aus fehlerhafter Installation, unsachgemäßem Betrieb sowie fehlerhafter Konfiguration ergeben. Der Hersteller behält sich das Recht vor, ohne vorherige Mitteilung Änderungen bezüglich Produkt, technischer Daten oder Montage- und Betriebsanleitung vorzunehmen.

VORSICHT	
	Einbau und Inbetriebnahme der VPN Appliance sollte nur von qualifiziertem Fachpersonal gemäß Bedienungsanleitung erfolgen. **Vor Inbetriebnahme ist die Unversehrtheit der VPN Appliance inklusive Zubehör sowie Anschlussleitungen sicherzustellen.**

VORSICHT	
	Die VPN Appliance darf nicht eingesetzt werden: ➢ in Umgebungen mit kondensierender Feuchtigkeit ➢ bei Umgebungstemperaturen unter 10°C oder über 45°C

4. Beschreibung des Gerätes

4.1. Bedienelemente der VPN Appliance

Das auf dieser Seite abgebildete System, zeigt die Standardversion einer VPN Appliance von msm net. Dabei handelt es sich um eine „Mini“ bzw. „Midi“ VPN Appliance in 19Zoll Bauform, geeignet für die Montage in einem Standard 19 Zoll Netzwerk-Rack (48,26 cm).

Diese Version hat auf der Vorderseite einen multifunktionalen Netzschalter. Als Kontrollelemente dienen die Netz-LED (grün) und die HDD-LED (rot). Die HDD-LED ist nur aktiv, wenn ein Datenzugriff auf den installierten Massenspeicher erfolgt.

Ist die VPN Appliance, wie abgebildet, für den Betrieb in einer Umgebung mit Smartcard-Authentifizierung vorgesehen, ist auf der Vorderseite ein Smartcard-Reader integriert.

Durch den Netzschalter werden folgende Funktionen realisiert:

Systemzustand	Funktion	Beschreibung
Ausgeschaltet	Systemstart	Durch einen kurzen Druck auf den Netzschalter wird das System gestartet. Die Betriebsbereitschaft wird dem Benutzer durch ein akustisches Signal gemeldet.
Eingeschaltet	Shutdown / System herunterfahren	Durch einen kurzes Betätigen des Netzschalters (< 1s), wird das System geordnet heruntergefahren und ausgeschaltet. Bei diesem Vorgang werden alle relevanten Daten gespeichert!
	Systemstopp	Durch ein längeres Betätigen des Netzschalters (> 2s) wird das System sofort ausgeschaltet. Bei diesem Vorgang können wichtige Daten verloren gehen.

VORSICHT	
	Durch ein längeres Betätigen des Netzschalters (> 2s) wird das System sofort ausgeschaltet. **Ein sofortiges Ausschalten des Systems, kann zum Verlust von wichtigen Daten führen.**

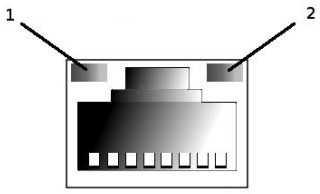
4.2. Anschlüsse auf der Rückseite der VPN Appliance

Die für den Betrieb notwendigen Anschlüsse der VPN Appliance sind grundsätzlich von der Konfiguration der für den konkreten Einsatzzweck geforderten Schnittstellen abhängig. Allen Geräten gemein ist jedoch folgende Grundausstattung:

- Stromversorgungsanschluss (ggf. sind die Einstellungen des Netzteils zu beachten)
- Internes Interface – LAN (in der Regel 1000Base-T Ethernet)
- Externes Interface – WAN (in der Regel 1000Base-T Ethernet; Andere mögliche Varianten sind: 1000BASE-Fiber, ATM, ISDN, DSL, GSM/UMTS oder Analog Modem)

NIC-Anzeigecodes:

Jede NIC auf der Rückseite hat eine integrierte Anzeige, die über den Zustand und den Verbindungsstatus der Netzwerkverbindung informiert.



1: Verbindungsanzeige 2: Aktivitätsanzeige

Anzeige	**Anzeigecodes**
Verbindungsanzeige und Aktivitätsanzeige leuchten nicht.	Die NIC ist nicht mit dem Netzwerk verbunden.
Verbindungsanzeige leuchtet in der Farbe rot/grün/gelb.	Die NIC ist mit dem Netzwerk verbunden die Datenrate ist 10/100/1000Mbit/s.
Die Aktivitätsanzeige blinkt gelb.	Die Netzwerkverbindung ist aktiv, es werden Daten gesendet oder empfangen.

HINWEIS	
	Alle weiteren Anschlüsse werden für den normalen Betrieb einer VPN Appliance nicht benötigt. Die Konfiguration erfolgt Remote über die integrierte Webschnittstelle.

4.3. Funktionsbeschreibung

Die msm net verfügt seit mehr als 10 Jahren über Erfahrungen im Einsatz und der Konzeption von VPN Lösungen. Unsere Produkte sind in den Bereichen Industrie, Handwerk und Behörden erfolgreich im Einsatz.

Besonderer Ausdruck der Leistungsfähigkeit unserer VPN Lösungen, ist eine Einsatzzulassung der deutschen Bundeswehr. Mit dieser Zulassung dürfen unsere VPN Appliances ohne weitere Überprüfung in der Sicherheitsstufe VS-NfD eingesetzt werden.

Ein Überblick zu den Parametern unserer VPN Appliances:

- Interoperabilität mit Standard VPN Routern wie z.B.: CISCO, Juniper Networks und VPN-Software-Clients z.B. von: CISCO, Microsoft, NCP
- VPN Protokolle wie IPSEC, L2TP und PPTP und Authentifizierung durch Zertifikate oder Pre-Shared Key werden unterstützt
- 2 und mehr VPN Appliances lassen sich als High Avaiability (HA) Cluster zusammenfassen
- mit Hilfe der NAT-Implementierung können über die VPN-Tunnel auch identische Subnetzadressen am Lokalen- und am Remote-Standort verbunden werden
- Card-Reader zum Einsatz von Smartcards mit Infinion-Chip und Siemens Card-OS M4.2 und M4.3
- X.509 Zertifikatsverwaltung inklusive PKI-Administration
- Eine schnörkellose Weboberfläche, die in den Experten Einstellungen dennoch den Zugriff direkt auf die Konfigurationsdateien ermöglicht
- Die Zertifikate für den Zugriff auf die Administrationsoberfläche lassen sich über die Konfigurationsoberfläche zuweisen
- Die Benutzerverwaltung kann auf der lokalen Appliance oder über das RADIUS-Protokoll erfolgen
- Systemaktualisierungen werden durch gesicherte Firmware-Updates bereitgestellt
- Unkomplizierte Sicherung und Wiederherstellung der Konfigurationsdaten
- Die VPN Appliances können direkt an einem DSL Modem betrieben werden
- Für größere VPN Netzwerke bieten wir zur leichteren Verwaltung zusätzlich Log- und Managementinfrastrukturdienste an

4.4. So erhalten Sie Unterstützung

Wir bieten Ihnen für Aufbau und Betrieb der VPN Infrastruktur folgende Hilfe und Unterstützung an:

- Projektierung, Planung und Realisierung von komplexen VPN Netzwerken und PKI Anwendungen
- Individuell auf unsere Kunden abgestimmte Service Level Agreements
- Beratungs- und Realisierungsleistungen zu Anwendungen und Systemeinführungen und -umstellungen
- Unterstützungsleistungen bei der Erarbeitung und Umsetzung von Konzeptionen und Organisationsumstellungen

Inhalt unserer Service Level Agreements:

Je nach den Erfordernissen (lokale Voraussetzungen und technischer Umfang) bieten wir Service- und Supportdienstleistungen in individuellen Serviceverträgen an. Wichtige Komponenten dieser SLA sind:

- Exklusive Bereitstellung von Updates für VPN Appliances
- Telefonsupport
- Remote- und Vor-Ort-Durchführung von Wartung- und Serviceleistungen
- Planung, Design und Implementierung von PKIs
- Aktive Überwachung und Administration von Kunden VPNs für die Unterstützung des Betriebes

Unsere Serviceverträge werden individuell mit unseren Kunden abgestimmt und realisiert.

Für weitergehende Fragen stehen wir Ihnen gern zur Verfügung.

Hersteller:	msm net meissner GmbH
Anschrift:	Greizer Strasse 87 D – 07937 Zeulenroda-Triebes Germany
Internet:	www.msm-net.de
E-Mail:	info@msm-net.de
Telefon:	+49 (0) 36628 9571-0
Fax:	+49 (0) 36628 9571-130

5. Einbauanleitung

5.1. Vorbereitung am Aufstellort

Die VPN Appliances sind für den Einbau in einem Standard Netzwerkschrank mit den Maßen 48,26cm (19 Zoll) Breite vorgesehen.

Bevor Sie das Gerät verwenden, prüfen Sie bitte ob folgende Voraussetzungen erfüllt sind:

VORSICHT	
	Stromversorgung: ➢ Die VPN Appliance sollte in der Nähe einer leicht zugänglichen Steckdose mit einer Wechselspannung von 110-240V bei 50-60Hz installiert werden. **Zugang:** ➢ Der Bediener sollte an der Vorder- und Rückseite ausreichend Bewegungsfreiheit haben. Auch Verkabelung, Stromanschlüsse und Belüftungsöffnungen sollten problemlos zugänglich sein. **Verkabelung:** ➢ Die Kabel sollten so sorgfältig verlegt und fixiert werden, dass elektromagnetische Einstreuungen durch Funksender, Funkverstärker, Stromleitungen sowie Leuchtmittel vermieden werden. **Umgebung:** ➢ Die Umgebungstemperatur darf nicht niedriger als +10°C oder höher als +45°C sein. ➢ Maximal 95% relative, nicht kondensierende Luftfeuchtigkeit

HINWEIS	
	Ist die VPN Appliance für den Einsatz von Smartcards vorgesehen, muss beim Einbau in einem 19 Zoll Rack auf genügend Abstand zur Fronttür geachtet werden.

5.2. Auspacken

Inhalt der Versandverpackung:

Kontrollieren Sie beim Auspacken der VPN Appliance, ob jeweils die folgenden Teile vorhanden sind:

- Eine VPN Appliance
- Ein Netzstromkabel
- Ein Montagekit für die Rack-Installation (zwei Montagehalter, Schrauben)
- Drucksachen:
  - „Bedienungsanleitung, Konfigurationsanleitung und technische Spezifikation für die VPN Appliance der msm net meissner GmbH“ (dieses Handbuch)
  - GPL Lizenz

Auspacken:

- Stellen Sie das Paket auf eine saubere, ebene Fläche und zerschneiden Sie die Paketklebebänder.
- Öffnen Sie die Verpackung und entfernen Sie die obere Abdeckung.
- Nehmen Sie die VPN Appliance vorsichtig aus der Verpackung und stellen Sie diese auf eine stabile, saubere Fläche.
- Entfernen Sie das gesamte Verpackungsmaterial.
- Untersuchen Sie das Produkt und das Zubehör auf Beschädigungen.

HINWEIS	
	Überprüfen Sie vor dem Auspacken der VPN Appliance, die Verpackung und melden Sie etwaige Beschädigungen unverzüglich an den Lieferanten.

5.2. Montage und Anschließen der VPN Appliance

Montage der VPN Appliance:

VORSICHT	
	Montage in einem Rack: Rack-Montagekits dürfen nicht dazu verwendet werden, die VPN Appliance unter einem Tisch, unter einer Platte oder an einer Wand zu befestigen. Trennen Sie bevor Sie fortfahren alle Kabel. Entfernen Sie gegebenenfalls alle selbstklebenden Unterlagen vom Boden der VPN Appliance. Wenn Sie mehrere 19-Zoll Geräte in einem Rack installieren, sollten Sie die Geräte mit dem Schwersten von unten beginnend nach oben einsetzen.

- Halten Sie einen der mitgelieferten Montagehalter an eine Seite der VPN Appliance. Dabei müssen die Montagebohrungen an der VPN Appliance mit den entsprechenden Bohrungen am Halter übereinstimmen.
- Führen Sie die mitgelieferten Schrauben in die Montagebohrungen am Halter ein und ziehen Sie diese mit einem Schraubendreher fest.
- Wiederholen Sie den Vorgang für den anderen Rackmontagehalter auf der gegenüberliegenden Seite der VPN Appliance.
- Setzen Sie die VPN Appliance im 19-Zoll-Rack (48,3cm) ein, wobei die Montagebohrungen am Gerät mit den entsprechenden Öffnungen am Rack zur Deckung kommen müssen.
- Befestigen Sie die VPN Appliance im Rack mit Rack-Schrauben oder mit Käfigmuttern und den entsprechenden Schrauben mit Unterlegscheibe (je nach Bauart des Racks). Ziehen Sie zuerst die unteren Schrauben und danach die oberen fest.

Anschließen der Verkabelung:

VORSICHT	
	Lesen Sie bitte aufmerksam die Sicherheitshinweise! Schließen Sie zuerst die informationstechnischen Kabel an, bevor Sie die Stromversorgung herstellen. Ein Nichtbeachten kann zu Defekten am Gerät und anderen Netzwerkkomponenten führen! Sobald die VPN Appliance mit Strom versorgt wird, beginnt der Bootvorgang.

Zum Minimieren von EMV-Störungen sollten für die informationstechnische Verkabelung möglichst hochwertige, geschirmte Patchkabel verwendet werden.

Die RJ45 Buchsen für den internen und für den externen Netzwerkzugang sind gekennzeichnet. Verbinden Sie diese mit den entsprechenden Geräten in Ihrem Netzwerk. Wenn alle Patchkabel angeschlossen sind, kann nun die Verbindung zum Stromnetz hergestellt werden.

5.3. Erstinbetriebnahme

Nachdem die VPN Appliance an ihrem Betriebsort aufgebaut und entsprechend der technischen Ausstattung verkabelt wurde, beginnt sofort nach dem Herstellen der Stromversorgung der Bootvorgang. Sollte das nicht der Fall sein, so wird sie durch ein kurzes Drücken des Netzschalters eingeschaltet.

Die VPN Appliance startet und bootet nach einem Selbsttest das System. Das Erreichen der Betriebsbereitschaft wird durch ein akustisches Signal gemeldet.

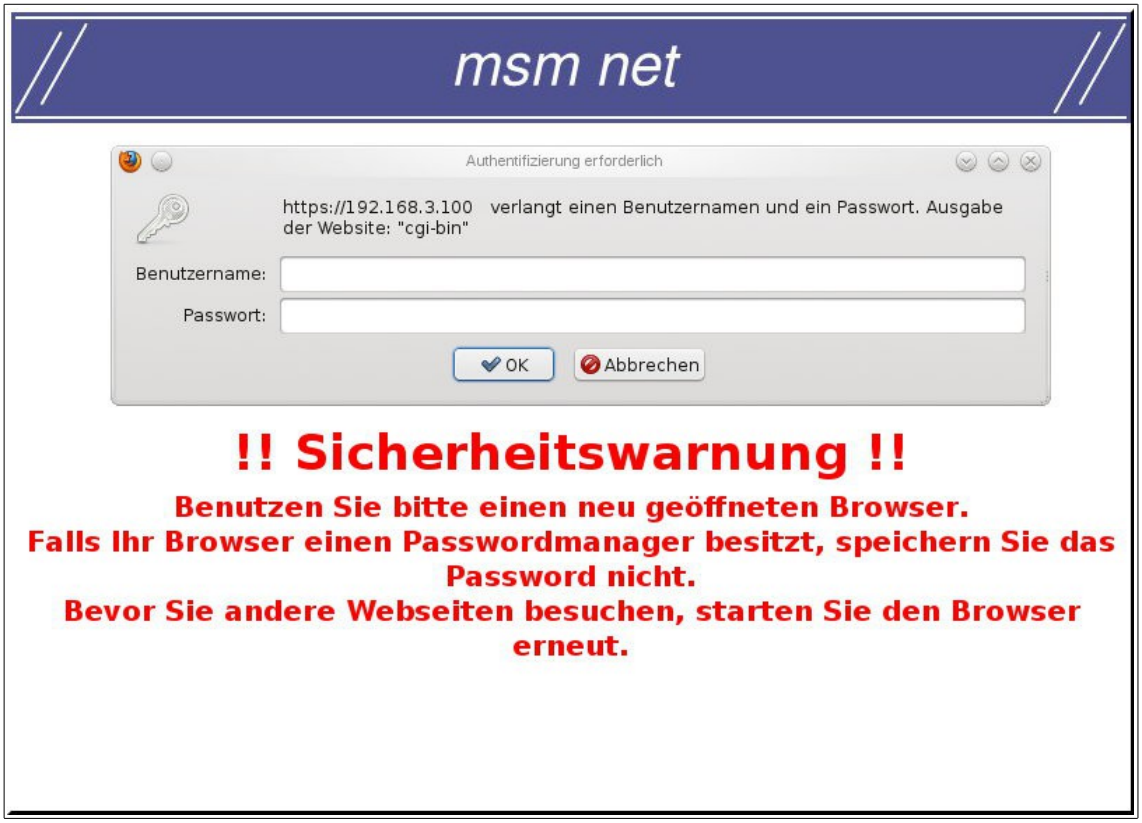
Um Zugriff auf die Konfigurationoberfläche der VPN Appliance zu erhalten müssen folgende Voraussetzungen erfüllt werden:

- Einen Arbeitsplatzrechner der mit dem internen Interface der Appliance verbunden ist.
- Im Auslieferungszustand ist die IP Adresse des Internen Interface der VPN Appliance auf 192.168.3.100/24 voreingestellt. Daher muss dem Arbeitsplatzrechner eine IP Adresse aus dem Subnetz 192.168.3.0/24 zugewiesen werden (mit Ausnahme 192.168.3.100).
- Geben Sie für den Zugriff auf die Konfigurationsoberfläche die Adresse https://192.168.3.100 in Ihren bevorzugten Browser ein.
- Für die erste Anmeldung verwenden Sie bitte „ADMINISTRATOR“ als Benutzername und „setup1“ als Passwort.
- Nach dem Log-in können Sie durch anklicken der Fahnen in der rechten oberen Ecke des Hauptmenüs zwischen den Sprachen Deutsch und Englisch wechseln.

Herzlichen Glückwunsch, Sie können jetzt mit dem Einrichten der VPN Appliance beginnen.

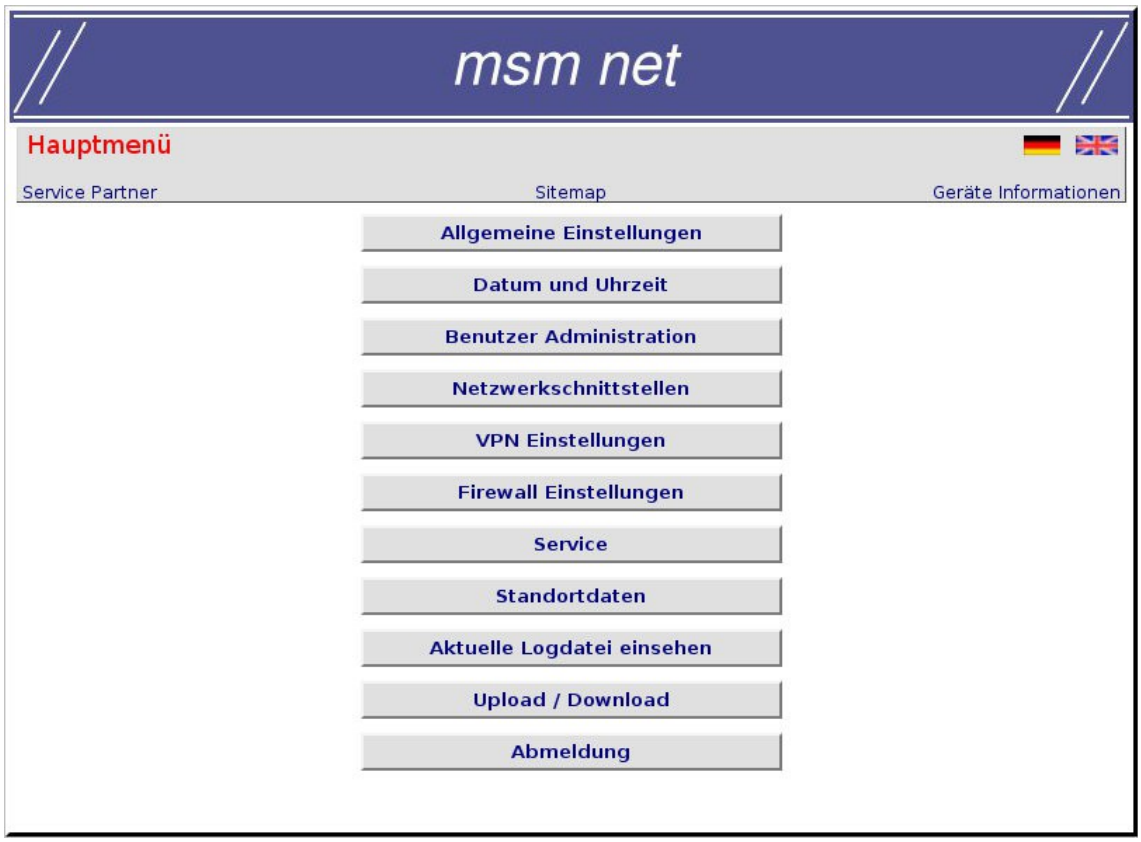
HINWEIS	
	Zugriff auf die VPN Appliance im Auslieferungszustand: ➢ Der Arbeitsplatzrechner von welchem die VPN Appliance konfiguriert werden soll, muss sich im Netzwerk des internen Interfaces befinden. In der Standardkonfiguration ist es das Netzwerk 192.168.3.0/24. ➢ IP Adresse internes Interface : 192.168.3.100/24 ➢ Benutzername: ADMINISTRATOR ➢ Passwort: setup1 Bitte beachten Sie, für Benutzername und Passwort ist die Groß-/Kleinschreibung zu beachten (case-sensitive). **Wird die VPN Appliance als Teil eines Projektes ausgeliefert, können für das Projekt andere Einstellungen definiert sein. Bitte beachten sie hierzu Ihre Projektunterlagen.**

Ist die VPN Appliance ordnungsgemäß installiert, wird mit Eingabe der vorgenannten IP-Adresse in Ihrem Browser folgender Begrüßungsbildschirm angezeigt.


msm net
Authentifizierung erforderlich
https://192.168.3.100 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "cgi-bin"
Benutzername:
Passwort:
OK
Abbrechen
!! Sicherheitswarnung !!
Benutzen Sie bitte einen neu geöffneten Browser.
Falls Ihr Browser einen Passwordmanager besitzt, speichern Sie das Password nicht.
Bevor Sie andere Webseiten besuchen, starten Sie den Browser erneut.

Das „Hauptmenü“:

Nach erfolgreicher Anmeldung wird folgendes Hauptmenü dargestellt.



6. Bedienung

Über das Hauptmenü sind alle relevanten Menüpunkte aufrufbar. Auf den folgenden Seiten werden die einzelnen Menüpunkte aufgezeigt und näher erklärt.

Die Weboberfläche der VPN Appliance hat eine klare Struktur. Generell sind die Konfigurationsparameter auf der linken Seite gelistet. Die Eingabefelder befinden sich in der Mitte und auf der rechten Seite eine kurze Erklärung.

Verschiedene Untermenüs bieten die Möglichkeit der Eingabe von Experten Einstellungen. In diesen Menüs können die Einstellungen direkt in den Konfigurationsdateien der VPN Appliance vorgenommen werden.

Für alle Einstellungen, die direkt in den Konfigurationsdateien vorgenommen werden können, sind unter dem Menüpunkt „Hilfe“ die entsprechenden originalen „Manpages“ aufrufbar. Diese „Manpages“ bieten einen detaillierten Überblick über die einzelnen Optionen der Konfigurationsdateien.

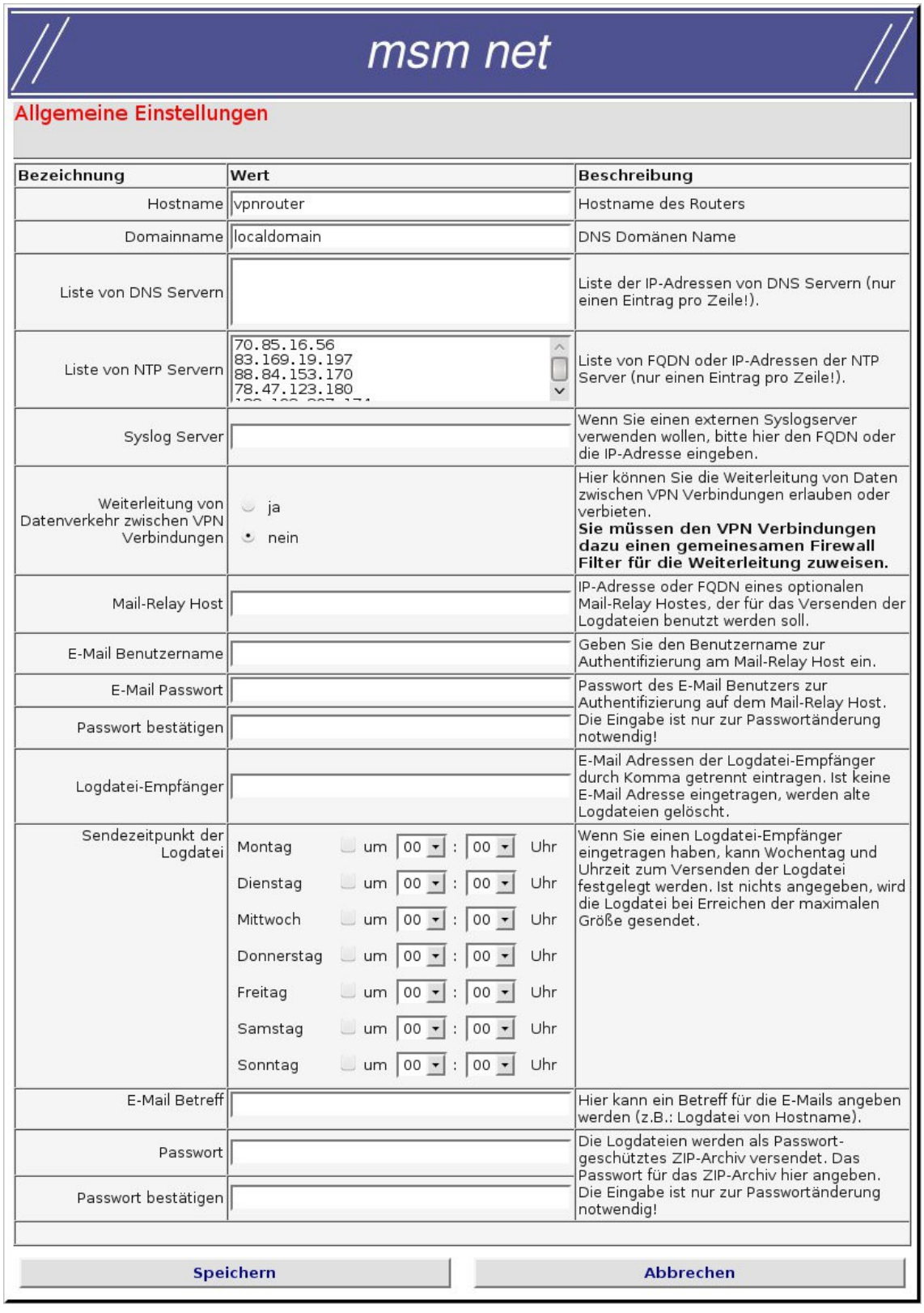
Über die „Sitemap“ können Sie sich jederzeit die Menüstruktur betrachten und direkt zu den einzelnen Untermenüs navigieren.

Unter dem Menüpunkt „Netzwerk“ können Sie, die für Ihr Netzwerk notwendigen Einstellungen vornehmen. Bitte beachten Sie, dass gegebenenfalls die geänderte Zugriffsadresse des internen Interfaces in Ihrem Browser neu eingegeben werden muss.

HINWEIS	
	Experten Einstellungen: ➢ Die in diesen Menüs vorgenommen Konfigurationseinstellungen haben direkte Auswirkung auf das Verhalten der jeweiligen Dienste. ➢ Die hier vorgenommenen Änderungen werden **nicht** auf mögliche Fehler überprüft! ➢ Bitte beachten Sie, falsche oder inkorrekte Optionen können Fehlfunktionen oder den Verlust von Daten hervorrufen. **Die Netzwerk-Interfaces:** ➢ Unter dem Menü „Netzwerkinterfaces“ können Sie, die für Ihr Netzwerk notwendigen Einstellungen vornehmen. ➢ Bitte beachten Sie, dass gegebenenfalls die geänderte Zugriffsadresse in Ihrem Browser eingegeben werden muss.

6.1. Allgemeine Einstellungen

Das Menü „Allgemeine Einstellungen“:


msm net
Allgemeine Einstellungen
Bezeichnung
Wert
Beschreibung
Hostname
vpnrouter
Hostname des Routers
Domainname
localdomain
DNS Domänen Name
Liste von DNS Servern
Liste der IP-Adressen von DNS Servern (nur einen Eintrag pro Zeile!).
Liste von NTP Servern
70.85.16.56
83.169.19.197
88.84.153.170
78.47.123.180
Liste von FQDN oder IP-Adressen der NTP Server (nur einen Eintrag pro Zeile!).
Syslog Server
Wenn Sie einen externen Syslogserver verwenden wollen, bitte hier den FQDN oder die IP-Adresse eingeben.
Weiterleitung von Datenverkehr zwischen VPN Verbindungen
ja
nein
Hier können Sie die Weiterleitung von Daten zwischen VPN Verbindungen erlauben oder verbieten.
Sie müssen den VPN Verbindungen dazu einen gemeinesamen Firewall Filter für die Weiterleitung zuweisen.
Mail-Relay Host
IP-Adresse oder FQDN eines optionalen Mail-Relay Hostes, der für das Versenden der Logdateien benutzt werden soll.
E-Mail Benutzername
Geben Sie den Benutzername zur Authentifizierung am Mail-Relay Host ein.
E-Mail Passwort
Passwort des E-Mail Benutzers zur Authentifizierung auf dem Mail-Relay Host. Die Eingabe ist nur zur Passwortänderung notwendig!
Passwort bestätigen
Logdatei-Empfänger
E-Mail Adressen der Logdatei-Empfänger durch Komma getrennt eintragen. Ist keine E-Mail Adresse eingetragen, werden alte Logdateien gelöscht.
Sendezeitpunkt der Logdatei
Montag um 00 : 00 Uhr
Dienstag um 00 : 00 Uhr
Mittwoch um 00 : 00 Uhr
Donnerstag um 00 : 00 Uhr
Freitag um 00 : 00 Uhr
Samstag um 00 : 00 Uhr
Sonntag um 00 : 00 Uhr
Wenn Sie einen Logdatei-Empfänger eingetragen haben, kann Wochentag und Uhrzeit zum Versenden der Logdatei festgelegt werden. Ist nichts angegeben, wird die Logdatei bei Erreichen der maximalen Größe gesendet.
E-Mail Betreff
Hier kann ein Betreff für die E-Mails angeben werden (z.B.: Logdatei von Hostname).
Passwort
Passwort bestätigen
Die Logdateien werden als Passwort-geschütztes ZIP-Archiv versendet. Das Passwort für das ZIP-Archiv hier angeben. Die Eingabe ist nur zur Passwortänderung notwendig!
Speichern
Abbrechen

6.2. Datum und Uhrzeit

Das Menü „Datum und Uhrzeit“:

HINWEIS	
	Wird im laufenden Betrieb die Zeiteinstellung geändert, kann es zu einer kurzen Unterbrechung der VPN Verbindungen kommen.

6.3. Benutzer Administration

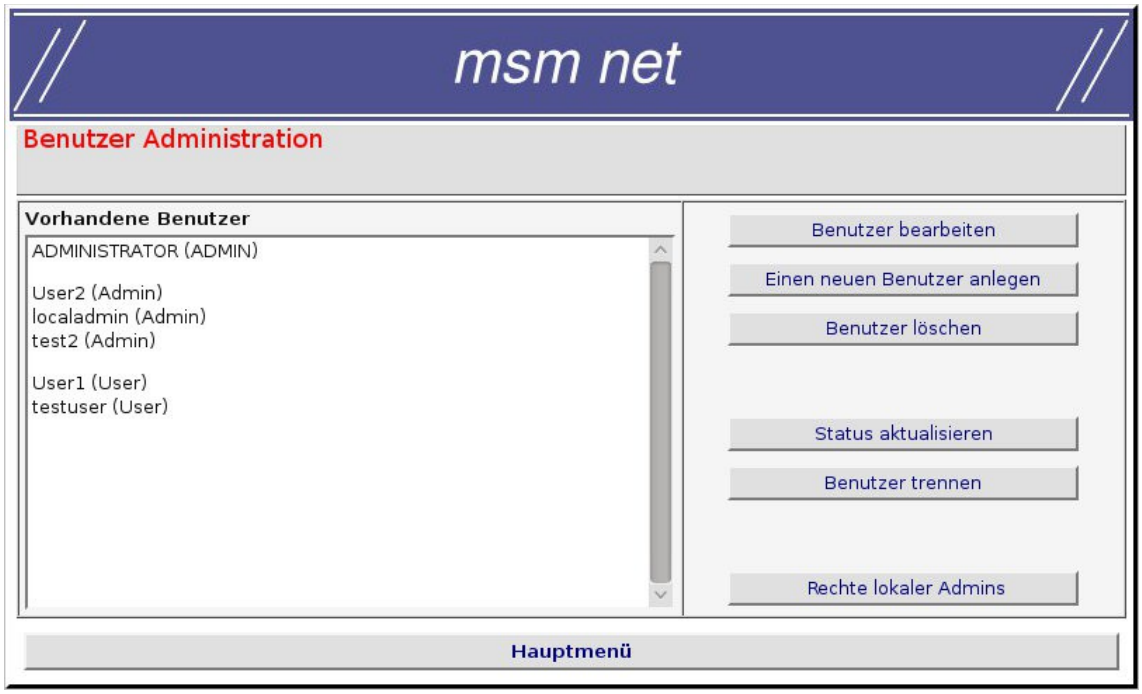
Für die Benutzerverwaltung unserer VPN Appliances greifen mehrere Komponenten ineinander. Zum Einen werden in der Benutzer- und in der Gruppenverwaltung die Berechtigungen für den Zugriff auf die Menüs der VPN Appliance festgelegt und zum Anderen kann über individuelle Firewall Regeln der Zugriff auf die Appliance selbst gesteuert werden.

Jedem Benutzer können in der Benutzerverwaltung individuelle Firewall Filter zugeordnet werden. Die Verwaltung der Firewall Filter erfolgt unter dem Menüpunkt „Firewall“ des Hauptmenüs.

Jedem Benutzer können außerdem spezifische Rechte zugewiesen werden, beispielsweise Gruppenzugehörigkeit, erlaubter Verbindungstyp oder die Erlaubnis zur Passwortänderung durch den Benutzer selbst.

Der Systemadministrator (ADMINISTRATOR) kann der Gruppe „Lokaler Administrator“ spezielle, anpassbare Berechtigungen zum Verwalten der Appliance zuordnen. Diese Berechtigungen gelten dann für alle Mitglieder dieser Gruppe. Im Menü „Benutzer Administration“ wird die Gruppenzugehörigkeit durch (Admin) für „Lokaler Administrator“ oder (User) für Standardbenutzer angezeigt.

Das Menü „Benutzer Administration“:



Das Menü „ Einen neuen Benutzer anlegen“:

Das Menü „Benutzer bearbeiten“:

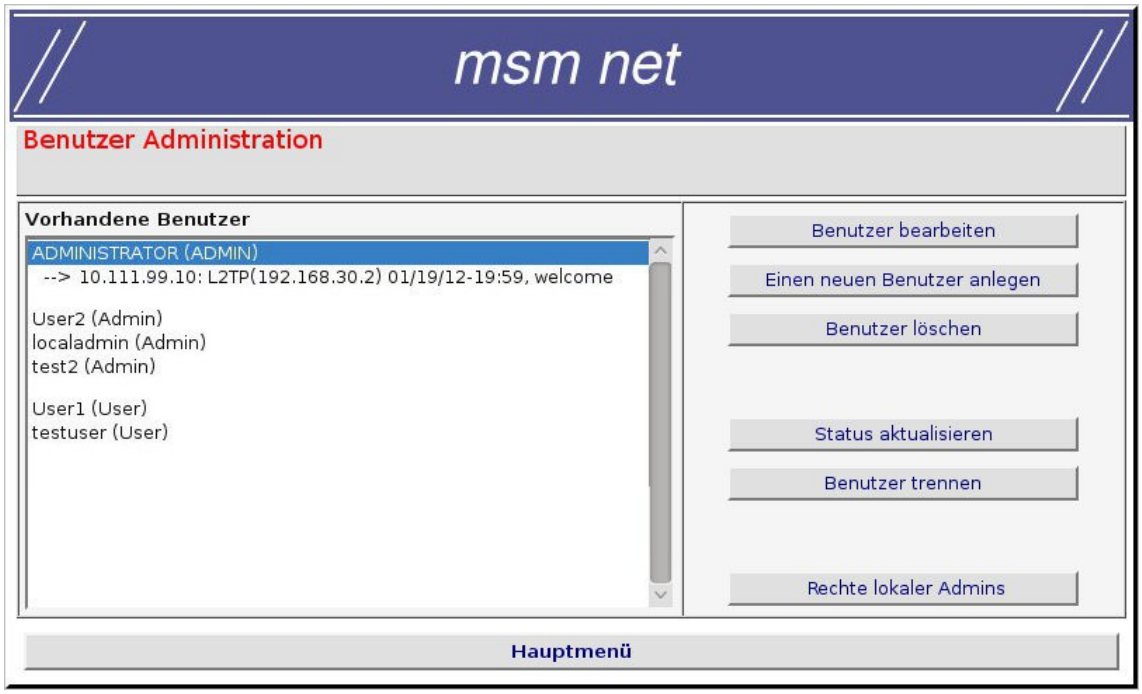
Das Löschen eines Benutzers

Wollen Sie einen Benutzer löschen, markieren Sie ihn zuerst im Menü „Benutzer Administration“. Mit einem Klick auf „Benutzer löschen“, wird nachstehende Warnung angezeigt. Durch eine weiteren Klick auf „Löschen“ wird die Aktion ausgeführt.

Die Warnmeldung „Benutzer löschen“:

Weitere Optionen des „Benutzer Administration” Menüs:

In dieser Abbildungen ist der Benutzer „ADMINISTRATOR” via L2TP mit der VPN Appliance verbunden.



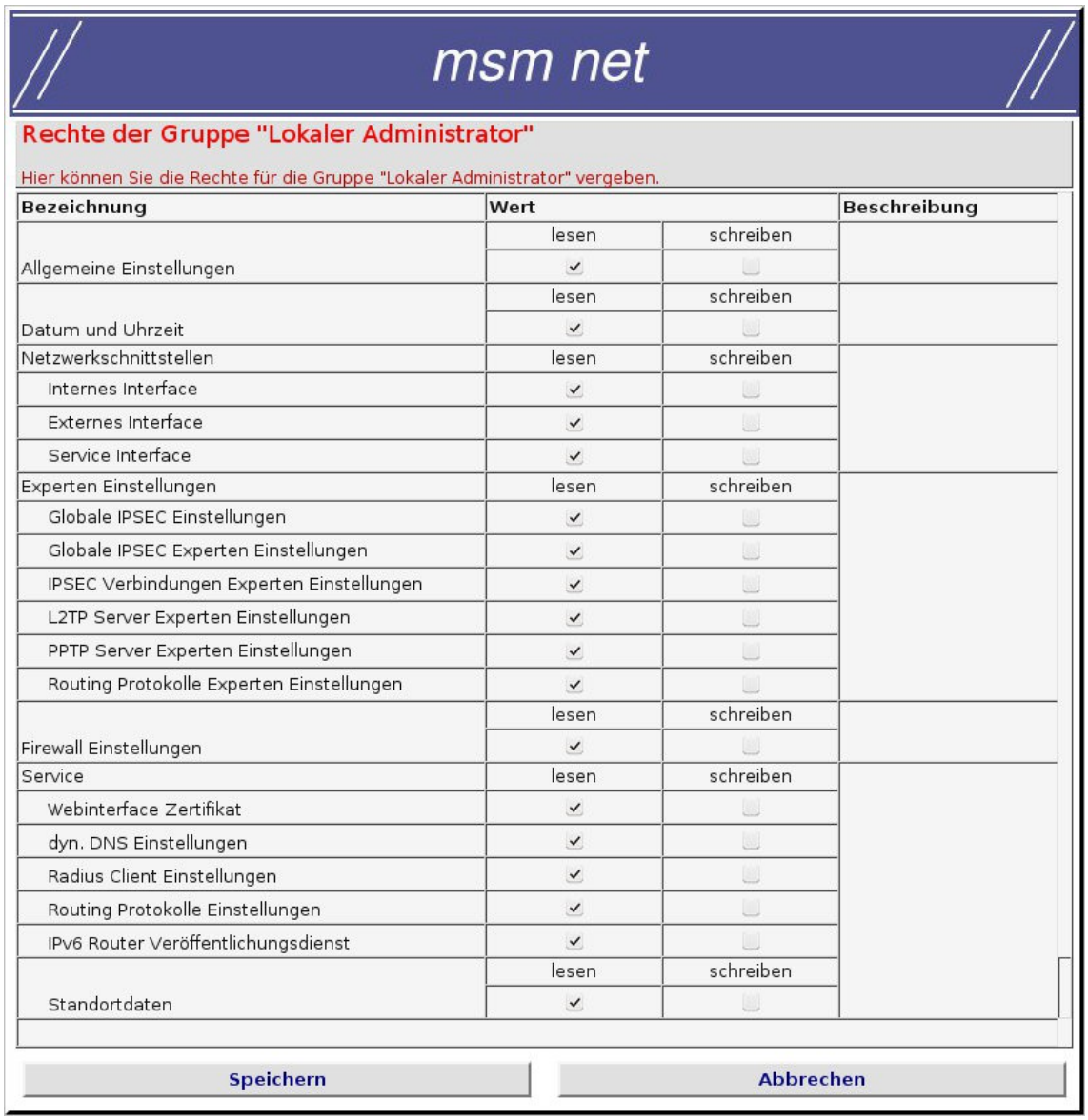
Die „Status aktualisieren” Schaltfläche

Sind Benutzer mit dem L2TP oder PPTP Server der VPN Appliance verbunden, werden zusätzliche Informationen angezeigt. Diese beinhalten die IP Adresse des Remote Hosts, die lokal zugewiesene IP Adresse, Verbindungszeit und den verwendeten Firewall Filter. Zum Aktualisieren der Statusanzeige klicken Sie auf „Status aktualisieren“.

Die „Benutzer trennen” Schaltfläche

Um einen markierten Benutzer zu trennen, betätigen Sie die Schaltfläche „Benutzer trennen”.

Das Menü „Rechte lokaler Admins“:



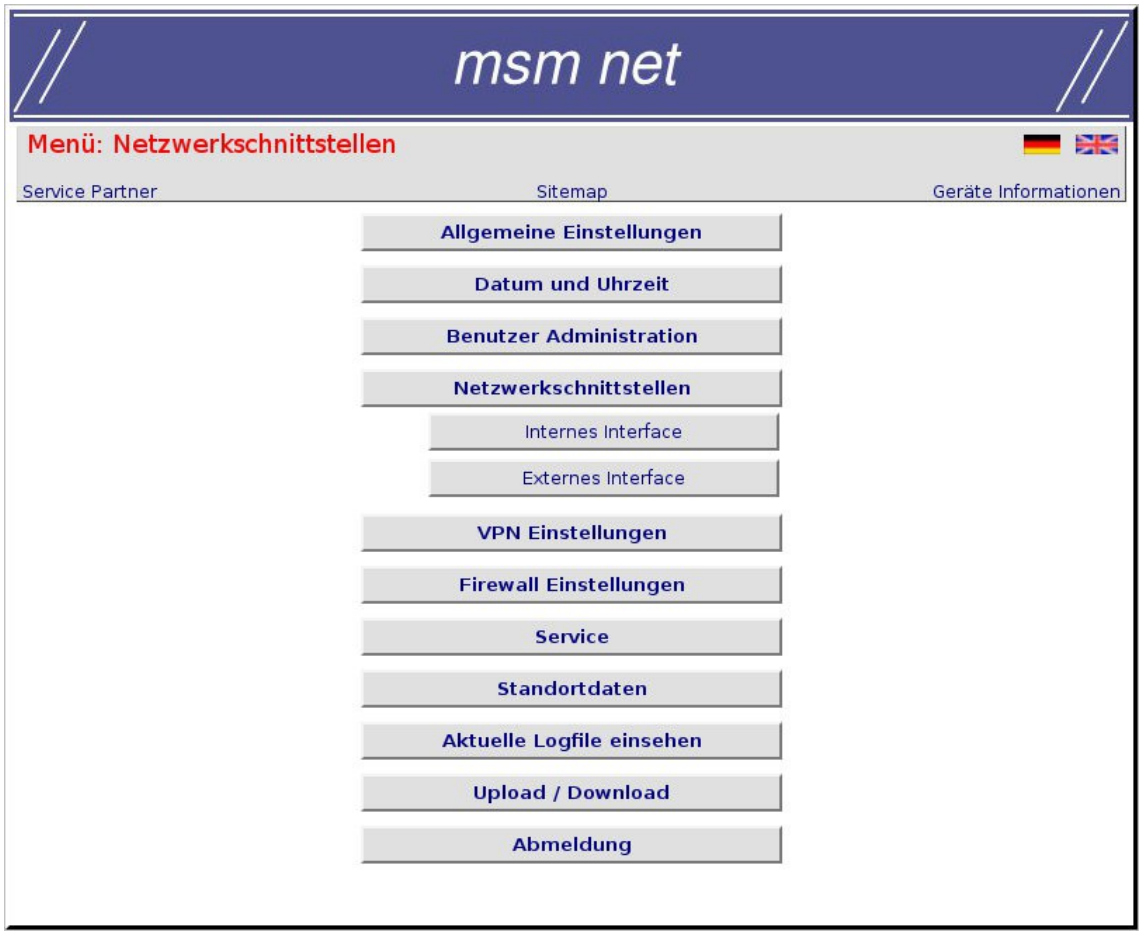
HINWEIS	
	Mitglieder der Gruppe „lokaler Administrator“ können in der Benutzer Verwaltung nur Einstellungen vornehmen, die sich auf die Mitglieder der Gruppe „User“ auswirken.

6.4. Netzwerkschnittstellen

Dieser Absatz beschreibt die Standardkonfiguration einer VPN Appliance, bestehend aus einem externen und einem internen Ethernet-Interface.

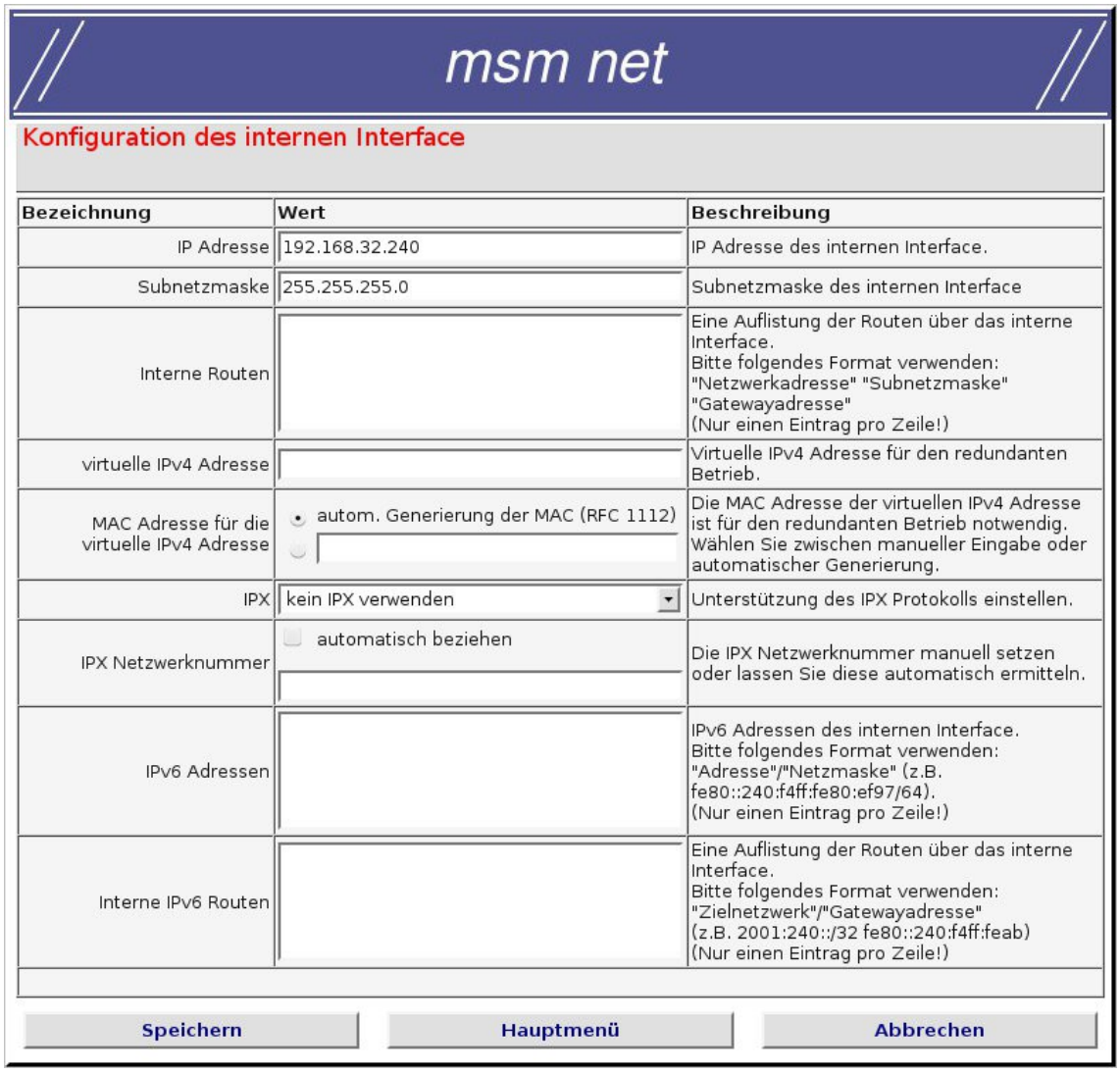
Im folgenden Menü kann das zu konfigurierende Interface ausgewählt werden.

Das Menü „Netzwerkschnittstellen“:

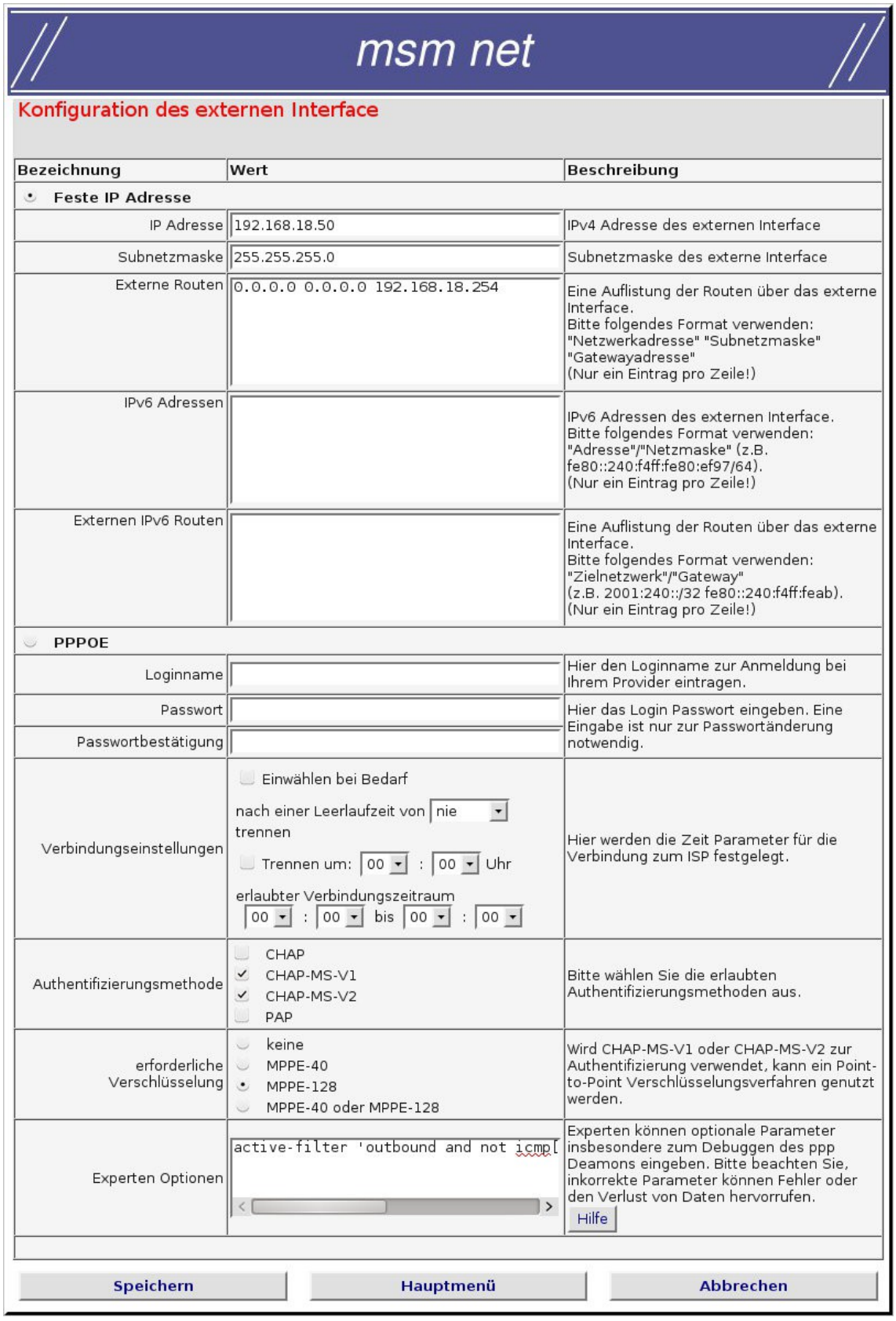


HINWEIS	
	Allgemein: ➢ Wurde die Netzwerkkonfiguration geändert, wird mit „Speichern“ die betreffende NIC neu gestartet. Dies führt zur Unterbrechung des Netzwerkverkehrs. ➢ Betrifft die Neukonfiguration die externe NIC, werden anschließend die aktiven VPN Verbindungen erneut etabliert. **Internes Interface:** ➢ Sollen IP Pakete zu internen Hosts geroutet werden, die sich nicht im Netzwerk des Internen Interface befinden, müssen Sie Routen zu diesen Hosts angeben. **Externes Interface:** ➢ Die Standardkonfiguration ist der Betrieb mit einer festen IP-Adresse. ➢ Für den Betrieb direkt an einem DSL Modem, kann PPPOE gewählt und konfiguriert werden.

6.4.1. Internes Interface (LAN)



6.4.2. Externes Interface (WAN)

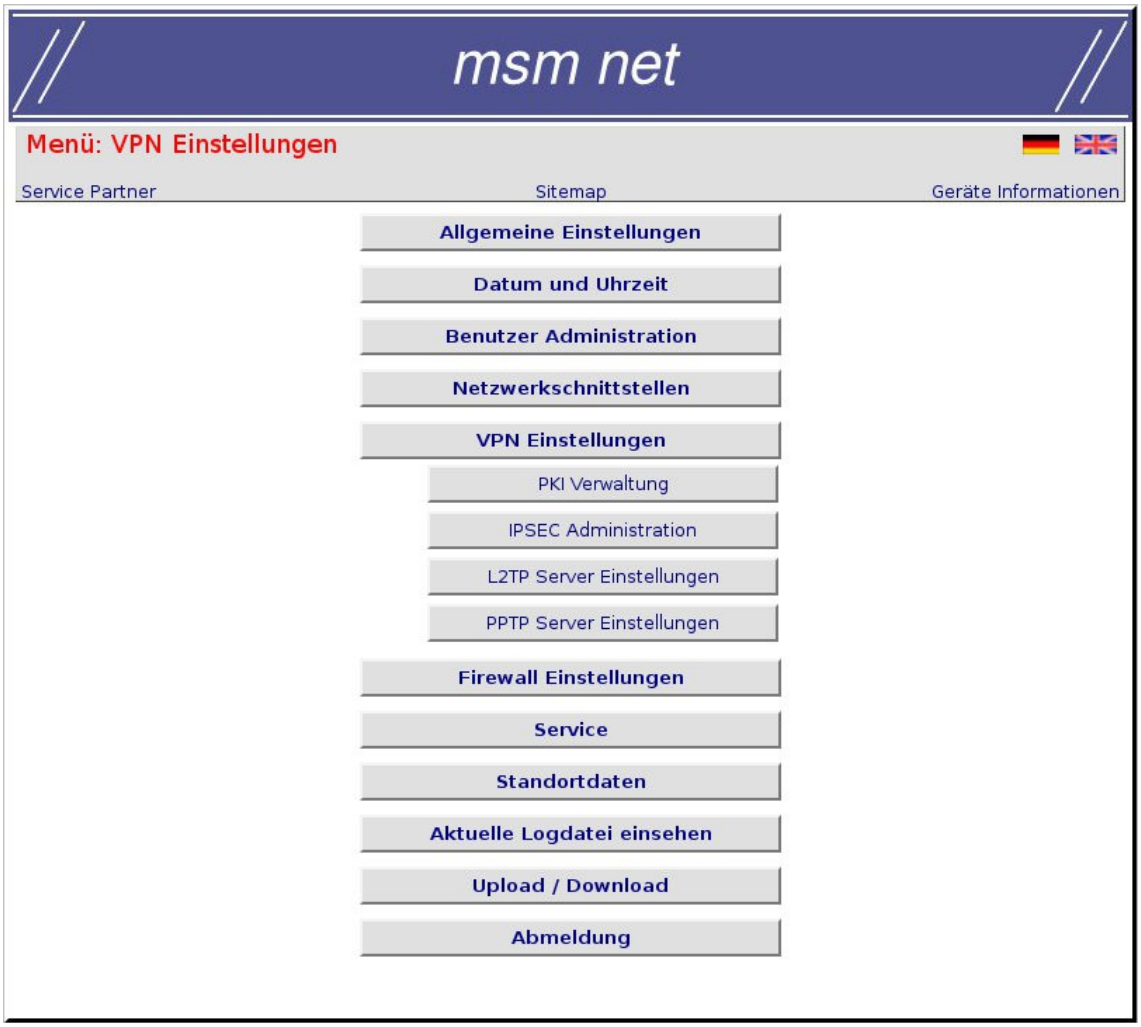


6.5. VPN Einstellungen

In diesem Kapitel wird beschrieben, wie VPN Verbindungen eingerichtet werden. Den Sicherheitsbedürfnissen Ihres Unternehmens entsprechend, können für die Authentifizierung der VPN Verbindungen X.509-Zertifikate oder „Pre-Shared Key“ eingesetzt werden.

Ein Werkzeug zur Erstellung und Administration von X.509 Zertifikaten ist in die Administrationsoberfläche der VPN Appliance integriert.

Das Menü „VPN Einstellungen“:



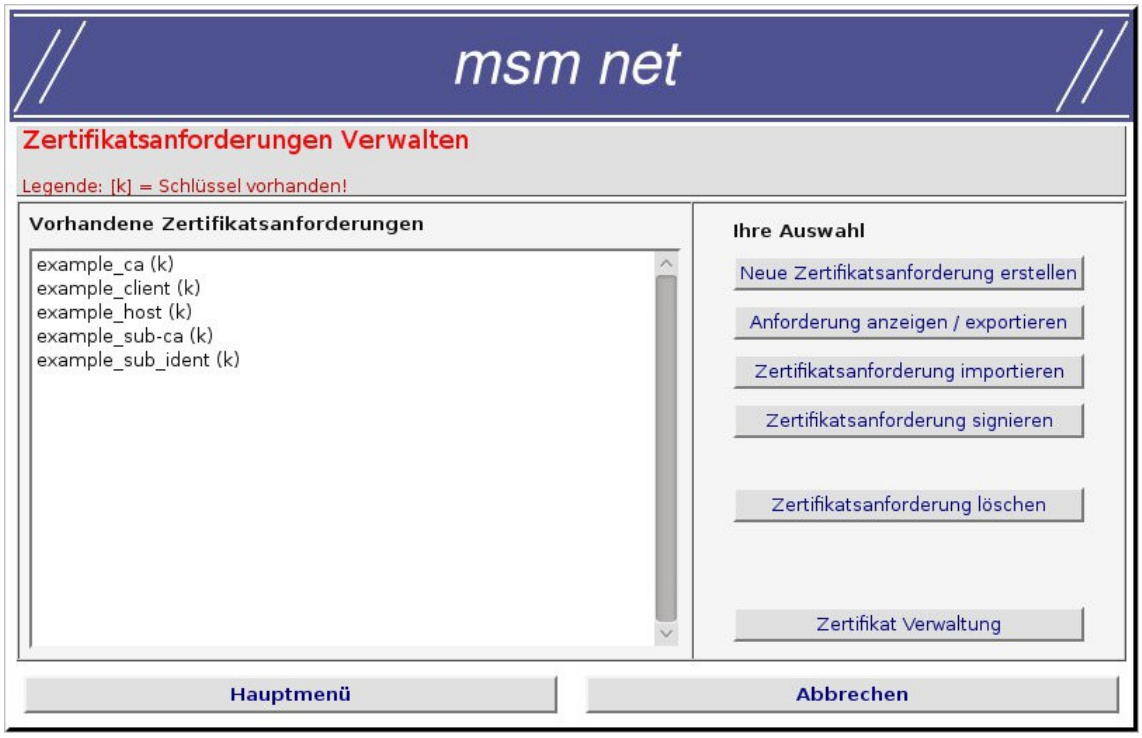
6.5.1. PKI Administration

Unter dem Menüpunkt „PKI Verwaltung“ sind alle Werkzeuge zur Verwaltung von Zertifikaten zusammengefasst.

Das Menü „PKI Verwaltung“:

6.5.1.1. Die Verwaltung von Zertifikatsanforderungen

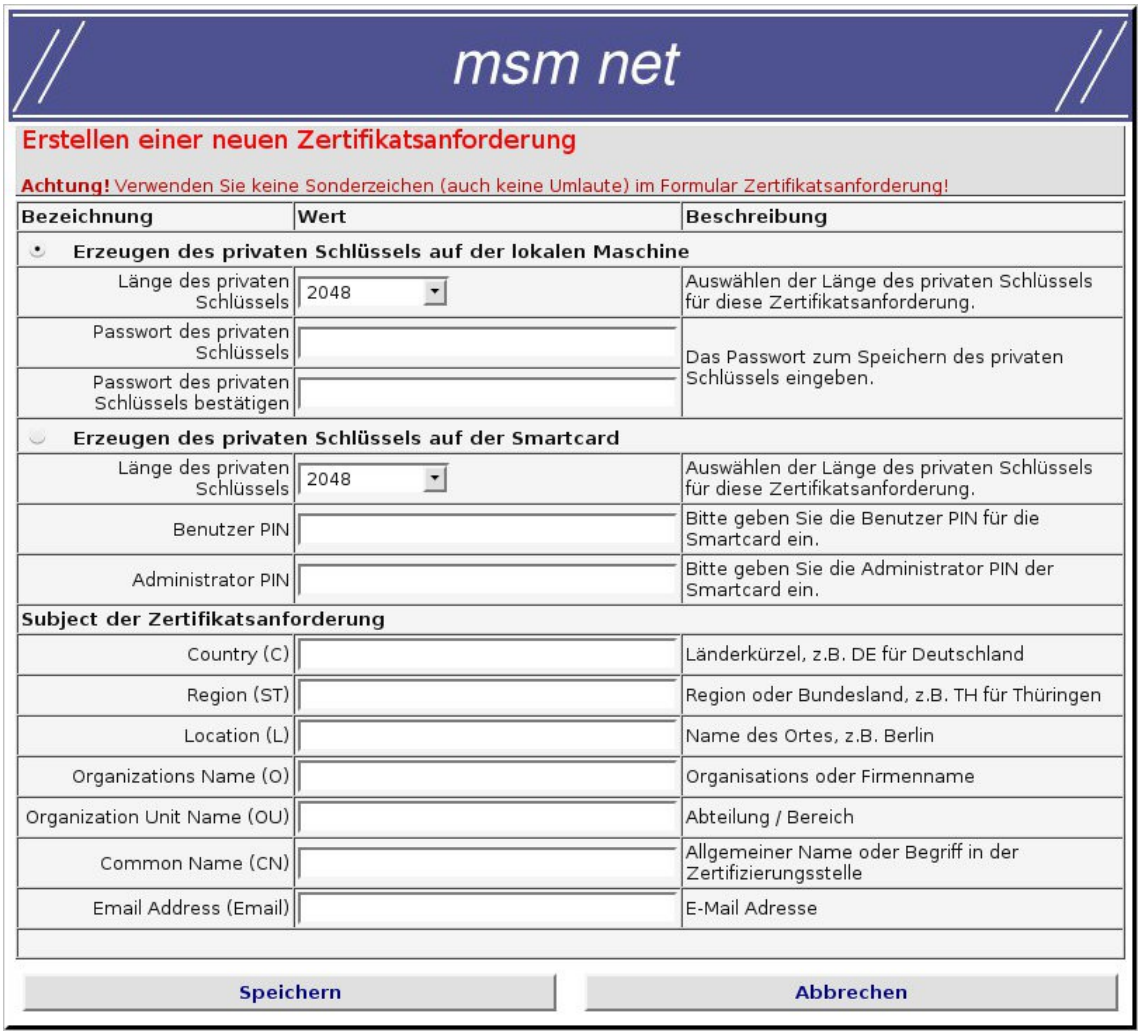
Das Menü „Zertifikatsanforderungen“:



Erstellen einer neuen Zertifikatsanforderung

Das Erstellen einer neuen Anforderung erfolgt über das Menü „Neue Zertifikatsanforderung erstellen“. Dabei ist das Erzeugen des privaten Schlüssels sowohl auf der lokalen Maschine, als auch auf einer im Card-Reader befindlichen Smartcard möglich. Wird eine Smartcard zur Schlüsselgenerierung verwendet, muss die Benutzer PIN und die Administrator PIN der Smartcard eingegeben werden.

Das Menü „Neue Zertifikatsanforderung erstellen“:


msm net
Erstellen einer neuen Zertifikatsanforderung
Achtung! Verwenden Sie keine Sonderzeichen (auch keine Umlaute) im Formular Zertifikatsanforderung!
Bezeichnung
Wert
Beschreibung
Erzeugen des privaten Schlüssels auf der lokalen Maschine
Länge des privaten Schlüssels
2048
Auswählen der Länge des privaten Schlüssels für diese Zertifikatsanforderung.
Passwort des privaten Schlüssels
Passwort des privaten Schlüssels bestätigen
Das Passwort zum Speichern des privaten Schlüssels eingeben.
Erzeugen des privaten Schlüssels auf der Smartcard
Länge des privaten Schlüssels
2048
Auswählen der Länge des privaten Schlüssels für diese Zertifikatsanforderung.
Benutzer PIN
Bitte geben Sie die Benutzer PIN für die Smartcard ein.
Administrator PIN
Bitte geben Sie die Administrator PIN der Smartcard ein.
Subject der Zertifikatsanforderung
Country (C)
Länderkürzel, z.B. DE für Deutschland
Region (ST)
Region oder Bundesland, z.B. TH für Thüringen
Location (L)
Name des Ortes, z.B. Berlin
Organizations Name (O)
Organisations oder Firmenname
Organization Unit Name (OU)
Abteilung / Bereich
Common Name (CN)
Allgemeiner Name oder Begriff in der Zertifizierungsstelle
Email Address (Email)
E-Mail Adresse
Speichern
Abbrechen

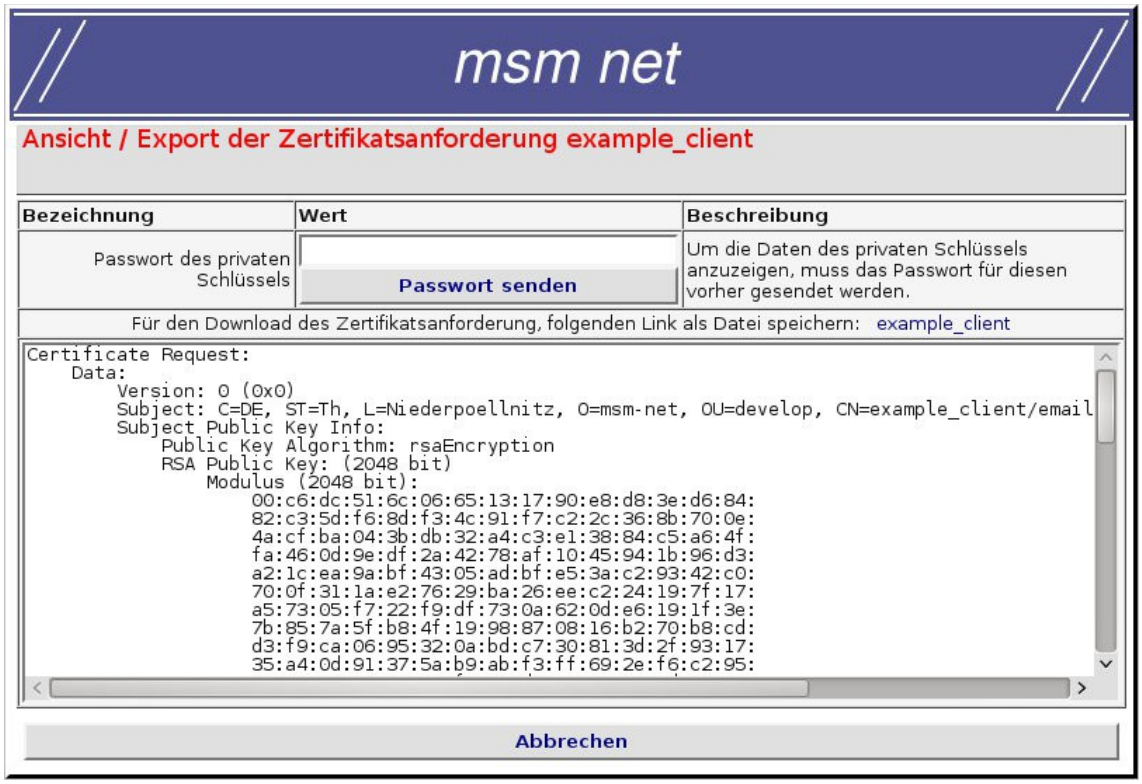
Ansehen und exportieren einer Zertifikatsanforderung

Wurde ein Request erstellt, kann er mit Hilfe dieser Maske überprüft werden. Nach dem Senden des Passwortes wird in dieser Maske ebenfalls der private Schlüssel angezeigt. Wurde die Zertifikatsanforderung mit einem privaten Schlüssel auf einer Smartcard erzeugt, kann der private Schlüssel nicht angezeigt oder exportiert werden.

Soll eine hier erzeugte Zertifikatsanforderung zum Signieren an eine Zertifizierungsstelle übertragen werden, erfolgt das ebenfalls mit dieser Maske.

Mit einem Klick der rechten Maustaste und der Option „Ziel speichern unter“ können sie die Zertifikatsanforderung auf einem lokalen Speichervolumen ablegen.

Das Menü „Anforderung anzeigen / exportieren“

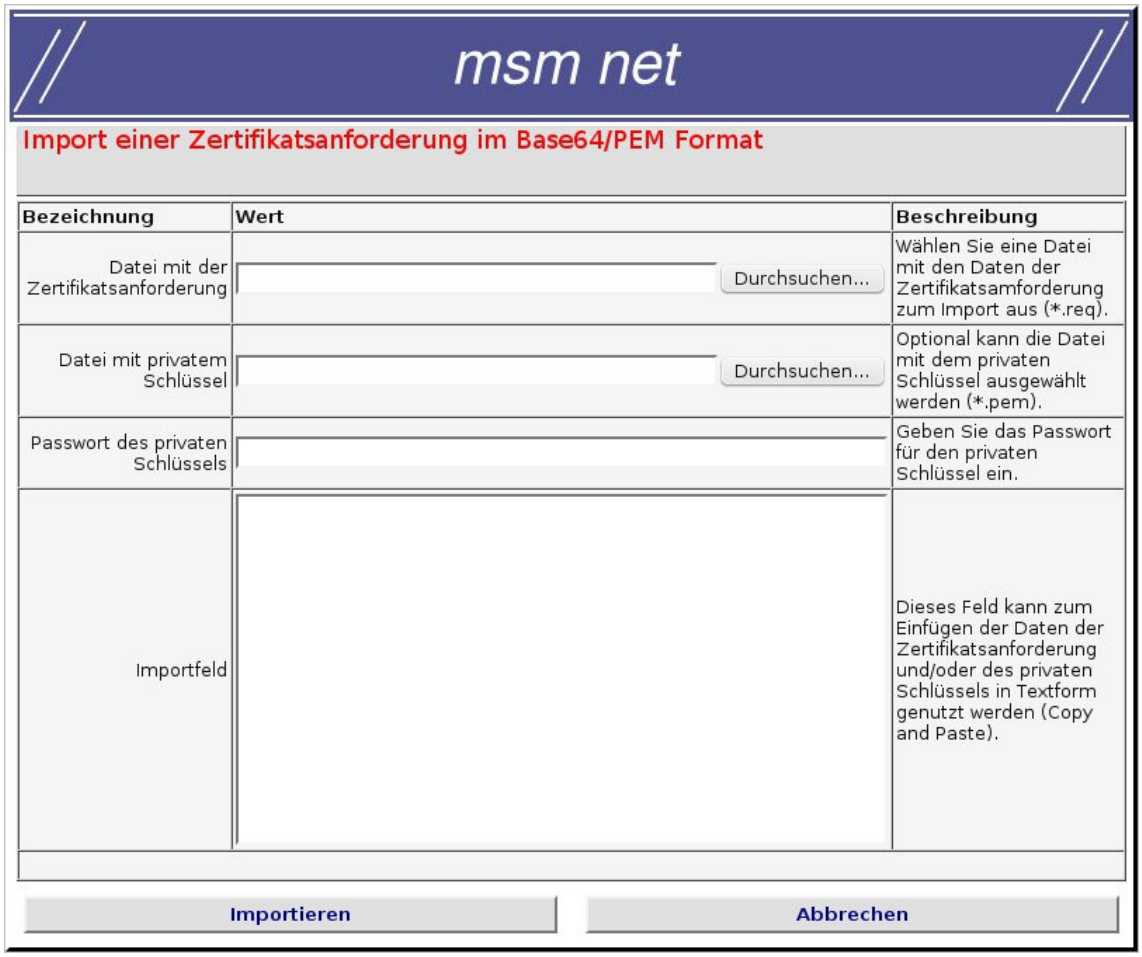


Importieren einer Zertifikatsanforderung

Mithilfe des Menüs können Sie eine extern generierte Zertifikatsanforderung im PEM kodierten Format importieren.

Für den Import können Sie entweder die entsprechenden Dateien auswählen oder mithilfe der „Copy and Paste“ - Funktion, die Daten in das Importfeld einfügen.

Das Menü „Zertifikatsanforderung importieren“:



Signieren einer Zertifikatsanforderung

Um ein Zertifikat aus einer Zertifikatsanforderung zu erzeugen, muss diese signiert werden. Zum Signieren der Anforderung, markieren Sie diese im Menü „Zertifikatsanforderungen“ und klicken Sie anschließend auf die Schaltfläche „Zertifikatsanforderung signieren“.

Es können 3 Arten von Zertifikaten erzeugt werden:

- ein (selbstsigniertes) Root-CA Zertifikat;
- ein Sub-CA Zertifikat;
- ein Identitäts-Zertifikat

Die Voraussetzug zum Erzeugen von Sub-CAs oder Identitäts-Zertifikaten ist das Vorhandensein einer Zertifizierungsstelle mit installiertem privaten Schlüssel.

Mit einem Klick auf die Schaltfläche „Signieren“ wird die Aktion ausgeführt.

Das Menü „Zertifikatsanforderung signieren“:

msm net
Signieren der Zertifikatsanforderung »example_client«
Bezeichnung
Wert
Beschreibung
Gültigkeit
Geben Sie die Gültigkeit des Zertifikates in Tagen, beginnend ab Signierung ein.
Signieren mit CA:
Ident. Zertifikat erstellen
Passwort/PIN für den privaten Schlüssel der CA
Mit dieser Option können Sie ein Ident-Zertifikat erstellen. Wählen Sie eine CA zum Signieren aus und geben Sie für den privaten Schlüssel das Passwort (oder die Benutzer PIN der Smartcard) ein.
Root-CA Zertifikat erstellen
Sub-CA Zertifikat erstellen
CA Zertifikat erstellen
Passwort/PIN des privaten Schlüssels
Primäre URL der CRL (optional)
Sekundäre URL der CRL (optional)
"Root-CA Zertifikat erstellen" zum Erzeugen einer selbssignierten Root-CA wählen und das Passwort des privaten Schlüssels der Zertifikatsanforderung eingeben.
Zum Erzeugen einer Sub-CA wählen Sie bitte eine CA aus und geben das Passwort für den privaten Schlüssel dieser CA ein.
Wenn der private Schlüssel auf einer Smartcard gespeichert wurde, bitte den Benutzer PIN der Smartcard eingeben.
Optional kann die URL für die CRL Verteilungspunkte in das CA Zertifikat integriert werden.
Signieren
Abbrechen

Löschen einer Zertifikatsanforderung

Wird eine Anforderung nicht mehr benötigt, kann diese im Menü Zertifikatsanforderungen gelöscht werden. Wählen Sie die entsprechende Anforderung und klicken Sie danach auf die Schaltfläche „Zertifikatsanforderung löschen“. Anschließend wird die nachfolgende Warnmeldung angezeigt. Die Aktion wird mit dem Betätigen der Schaltfläche „Anfoderung löschen“ unwiderruflich ausgeführt.

Die Warnmeldung „Zertifikatsanforderung löschen“

Zur Zertifikat Verwaltung wechseln

Durch das Anklicken der Schaltfläche „Zertifikat Verwaltung“ des Zertifikatsanforderungen-Menüs, können Sie direkt zum Menü „Zertifikat Verwaltung“ wechseln.

6.5.1.2. Das Verwalten von Zertifikaten

Das Menü „Zertifikat Verwaltung“ stellt auf der linken Seite alle vorhandenen Zertifikate in ihrer direkten Abhängigkeit zu vorhandenen Zertifizierungsstellen dar. Im Beispiel der Abbildung ist unter der Root-CA „exaple_ca“ die verfügbare Sub-CA „example_sub-ca“ gelistet. Die Ident.-Zertifikate, die von der Sub-CA ausgestellt wurden, sind unter der Sub-CA selbst gelistet.

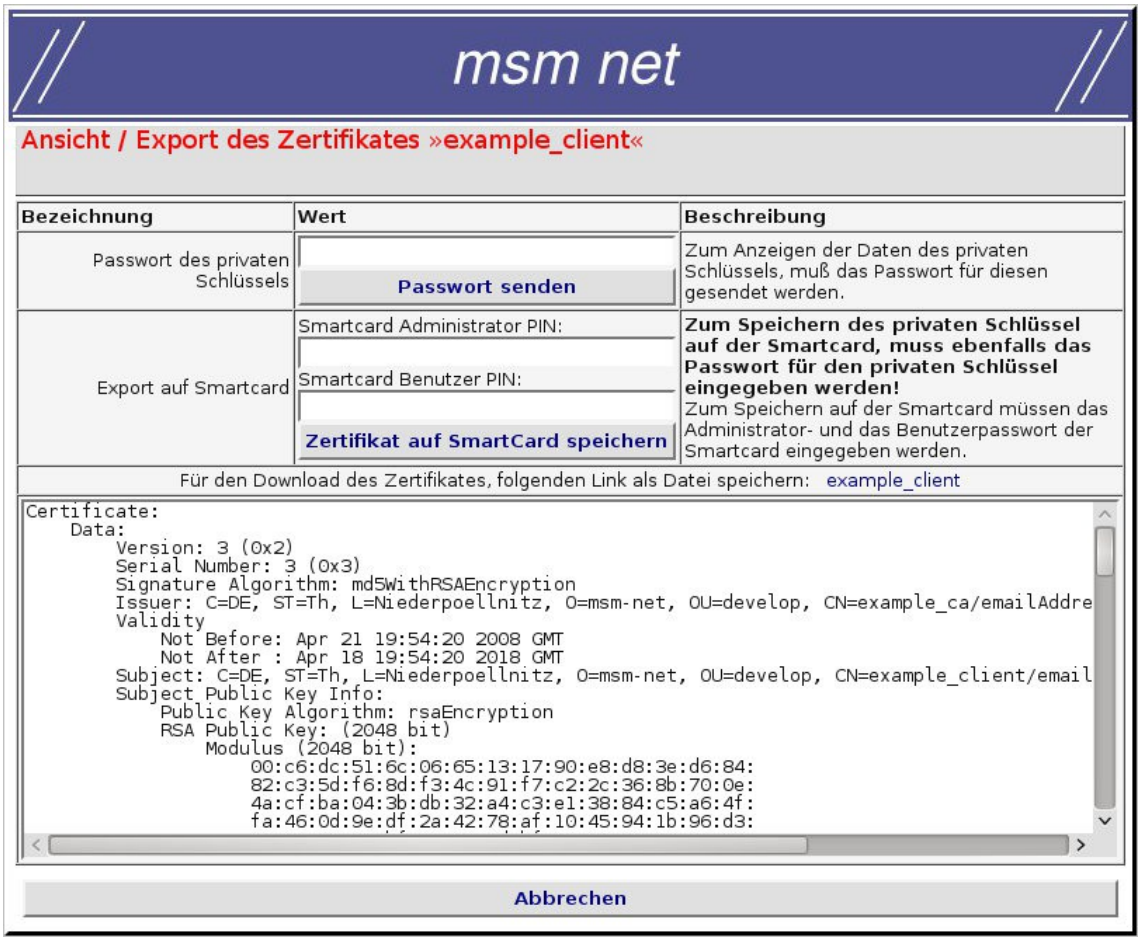
Auf der rechten Seite sind im Menü alle Werkzeuge zum Bearbeiten von Zertifikaten angeordnet. Wenn, mit Ausnahme eines Importvorganges, eine Aktion durchgeführt werden soll, so ist vor dem Klicken einer Schaltfläche erst im linken Bereich ein Objekt, auf das die Aktion angewendet werden soll, auszuwählen. Ist die Aktion für das gewählte Objekt nicht möglich, wird eine Fehlermeldung angezeigt.

Wenn der private Schlüssel für eine CA vorhanden ist, kann für diese eine Certificate Revocation List (CRL) erstellt und verwaltet werden. Zusätzlich wird ein Update der CRL zum Zurückziehen/Löschen für die von dieser CA signierten Zertifikaten erstellt.

Ist für eine CA kein Schlüssel vorhanden, kann eine CRL lediglich importiert und verwendet werden.

Das Menü „Zertifikat Verwaltung“:

Das Menü „Zertifikat anzeigen / exportieren“:

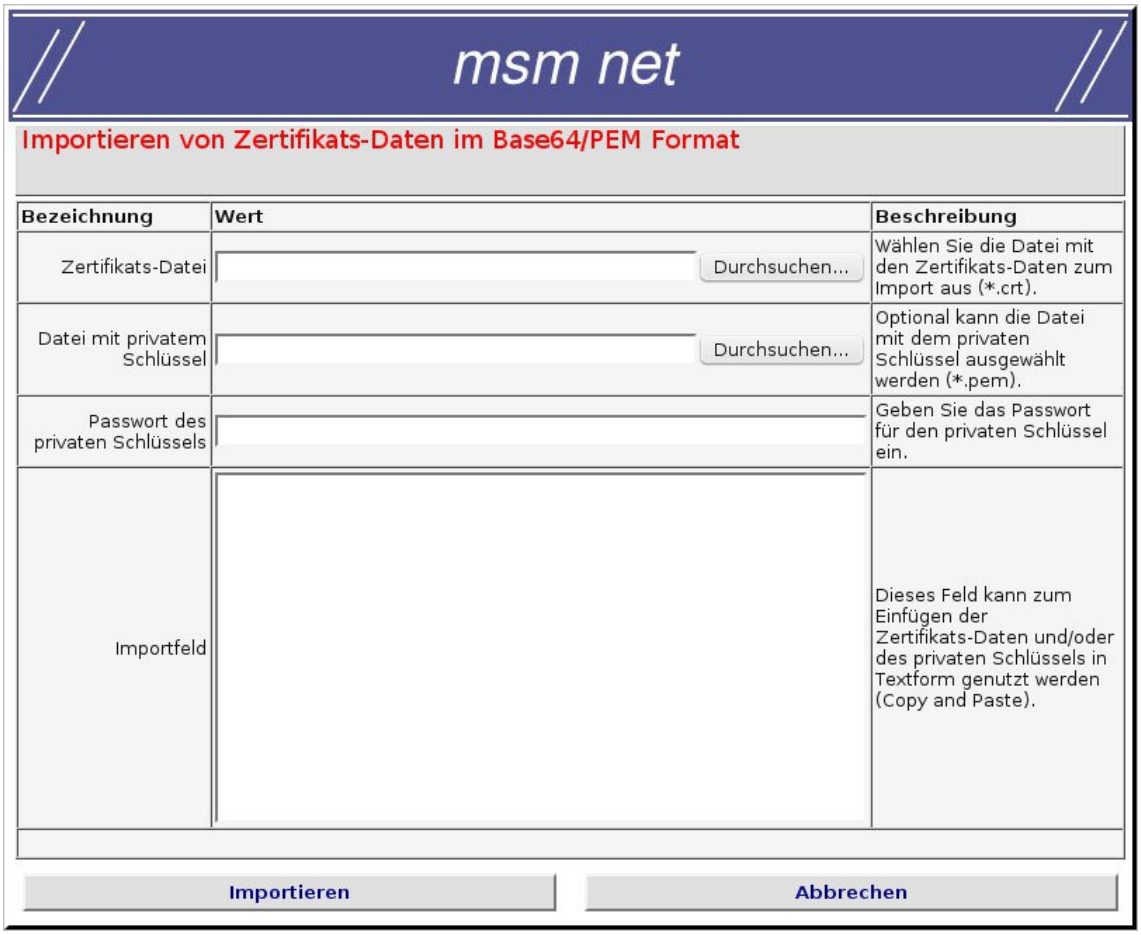

msm net
Ansicht / Export des Zertifikates »example_client«
Bezeichnung
Wert
Beschreibung
Passwort des privaten Schlüssels
Passwort senden
Zum Anzeigen der Daten des privaten Schlüssels, muß das Passwort für diesen gesendet werden.
Export auf Smartcard
Smartcard Administrator PIN:
Smartcard Benutzer PIN:
Zertifikat auf SmartCard speichern
Zum Speichern des privaten Schlüssel auf der Smartcard, muss ebenfalls das Passwort für den privaten Schlüssel eingegeben werden!
Zum Speichern auf der Smartcard müssen das Administrator- und das Benutzerpasswort der Smartcard eingegeben werden.
Für den Download des Zertifikates, folgenden Link als Datei speichern: example_client
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 3 (0x3)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=DE, ST=Th, L=Niederpoellnitz, O=msm-net, OU=develop, CN=example_ca/emailAddre
Validity
Not Before: Apr 21 19:54:20 2008 GMT
Not After : Apr 18 19:54:20 2018 GMT
Subject: C=DE, ST=Th, L=Niederpoellnitz, O=msm-net, OU=develop, CN=example_client/email
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:c6:dc:51:6c:06:65:13:17:90:e8:d8:3e:d6:84:
82:c3:5d:f6:8d:f3:4c:91:f7:c2:2c:36:8b:70:0e:
4a:cf:ba:04:3b:db:32:a4:c3:e1:38:84:c5:a6:4f:
fa:46:0d:9e:df:2a:42:78:af:10:45:94:1b:96:d3:
Abbrechen

HINWEIS	
	Validity / Gültigkeit eines Zertifikates: ➢ Ist ein Zertifikat abgelaufen oder noch nicht gültig, kann mit diesem Zertifikat keine Verbindung authentifiziert oder etabliert werden!

Importieren eines Zertifikates

Ist in Ihrem Unternehmen schon eine PKI vorhanden oder sollen von einer anderen CA signierte Zertifikate verwendet werden, können diese Zertifikate importiert werden.

Das Menü „Zertifikat importieren“:



PKCS12 Export / Import

PKCS12 definiert ein verbreitetes Dateiformat, welches zum Speichern von X.509 Zertifikaten und privaten Schlüsseln dient. Das Dateiformat wird dabei durch eine Kennwort basierte symmetrische Verschlüsselung geschützt.

Wird ein Zertifikat über die PKCS12-Exportfunktion exportiert, werden alle Zertifikate der Zertifizierungskette und falls verfügbar auch der private Schlüssel des Zertifikates in der PKCS12-Datei gespeichert.

Wenn eine PKCS12-Datei importiert werden soll, müssen Sie darauf achten, dass nur der private Schlüssel des letzten Zertifikates der Zertifizierungskette enthalten ist.

Das Menü „Zertifikat exportieren (PKCS12)“:

Das Menü „Zertifikat importieren (PKCS12)“:

Löschen/widerrufen eines installierten Zertifikates:

Wird ein Zertifikat nicht mehr benötigt, kann es in der Zertifikatsverwaltung gelöscht werden. Markieren Sie zuerst das entsprechende Zertifikat in der Liste und klicken Sie danach auf die „Zertifikat löschen“ Schaltfläche. Anschließend wird eine Warnmeldung angezeigt.

Bei der unten abgebildeten Warnmeldung handelt es sich um die Variante für eine lokal verwaltet CA (der private Schlüssel der CA ist installiert). Mit der Eingabe des CA Passwortes und der Gültigkeitsdauer für die CRL wird nach dem Bestätigen das Zertifikat gelöscht und ein Update der CRL erstellt.

Wenn Sie ein Zertifikat löschen wollen, welches nicht auf dieser Appliance verwaltet wird, werden die Eingabefelder für das CA Passwort und die Gültigkeitsdauer in der Warnmeldung nicht angezeigt. Nach dem Bestätigen wird nur das Zertifikat von der lokalen Maschinen gelöscht.

Durch klicken auf die Schaltfläche „Sperren / Löschen“ wird die Aktion ausgeführt.

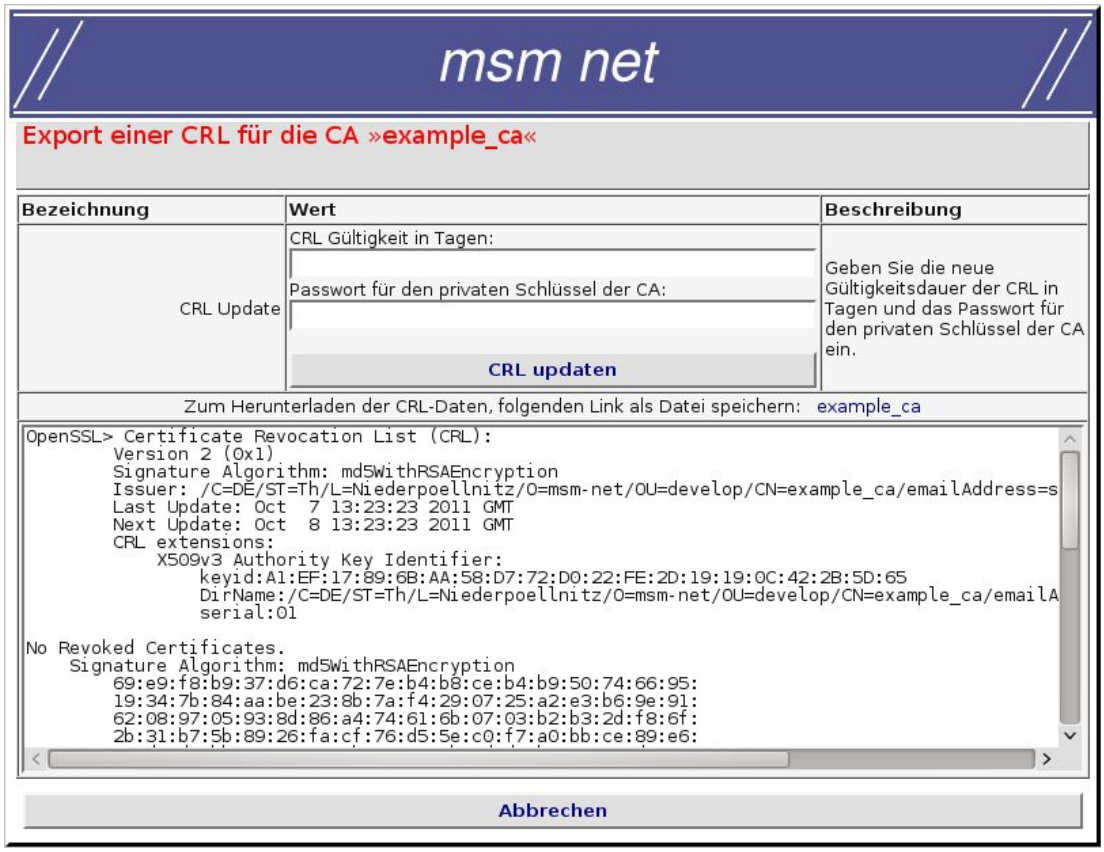
Die Warnmeldung „Zertifikat löschen“:

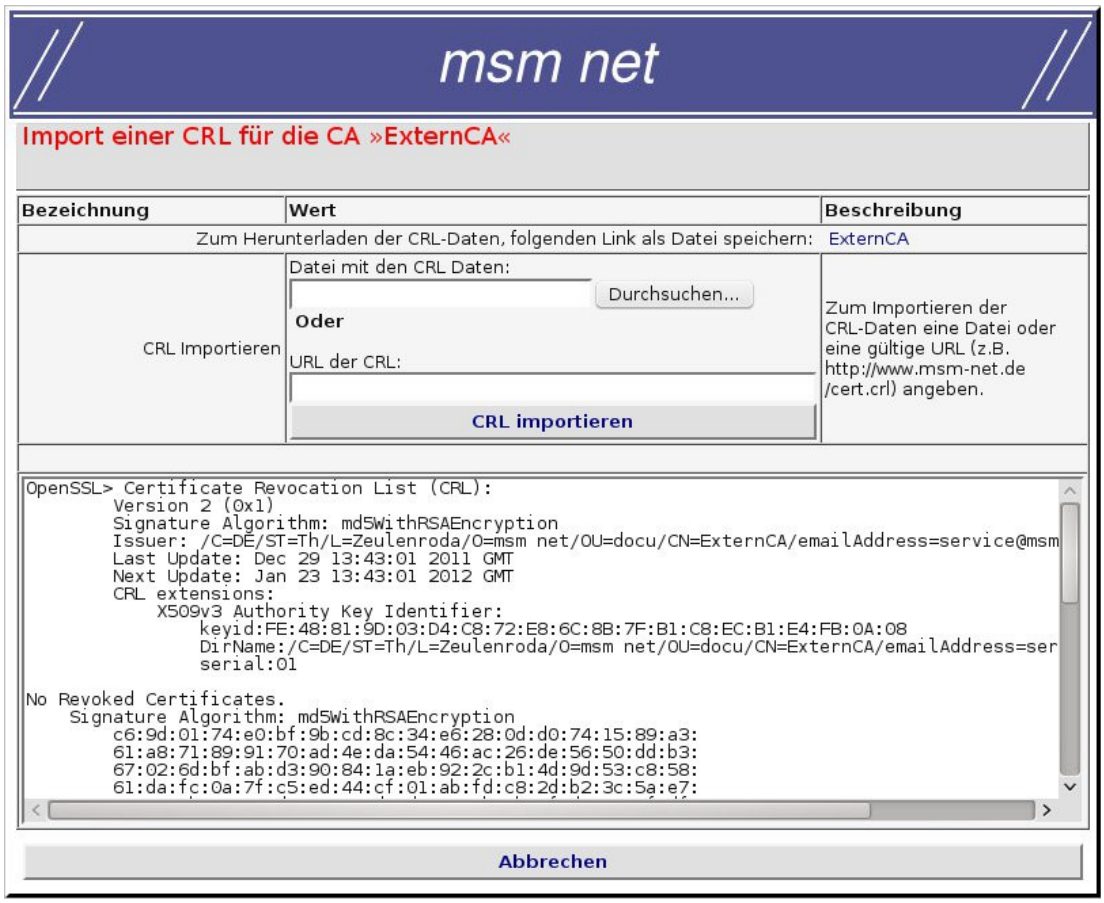
msm net
Löschen / Sperren des Zertifikates »example_client«
!! Warnung !!
Das Löschen / Sperren des Zertifikates erfolgt permanent.
Wenn Sie sicher sind, dann fahren Sie fort.
Passwort des privaten Schlüssels der CA example_ca:
Neue Gültigkeitsdauer der CRL in Tagen:
Sperren / Löschen
Abbrechen

Das Menü „CRL Einstellungen für IPSEC“:

Das Menü „CRL Verwalten“:

Davon abhängig ob Sie eine extern oder eine lokal verwaltete CA wählen, wird das „CRL Verwalten“ Menü einer der beiden Abbildungen entsprechen.





HINWEIS	
	Verwalten von „Certificate Revocation Lists“: ➢ Ist der private Schlüssel einer CA vorhanden, kann eine Certificate Revocation List erstellt, verwaltet und exportiert werden. ➢ Ist kein privater Schlüssel vorhanden, kann eine CRL lediglich importiert werden.

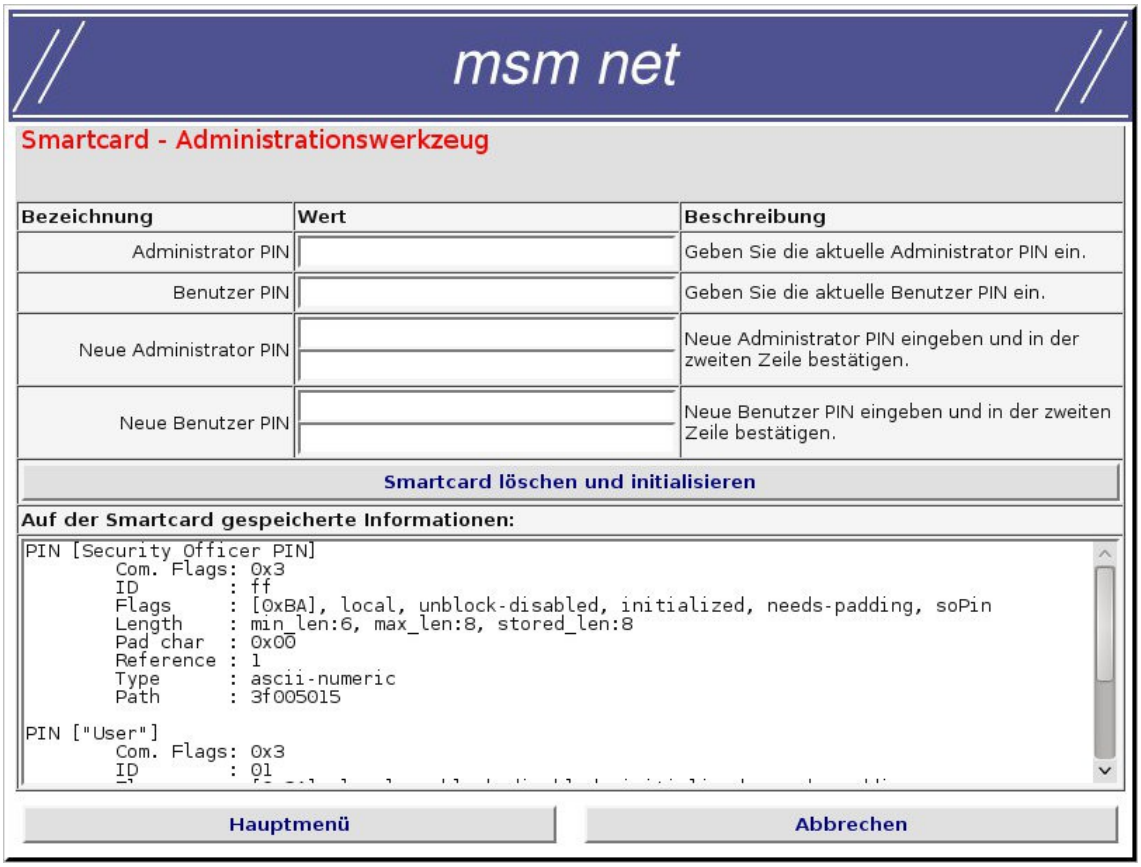
Zur Menü Zertifikatsanfoderungen wechseln

Durch das Anklicken der Schaltfläche „Zertifikatsanforderungen Verwalten“ der Zertifikatsverwaltung, können Sie direkt zum Menü „Zertifikatsanforderungen Verwalten“ wechseln.

6.5.1.3. Die Verwaltung von Smartcards

Mithilfe des Smartcard Werkzeugs, können die Verwaltungsaufgaben initialisieren und reinitialisieren einer Smartcard durchgeführt werden. Bei diesen Vorgängen werden sowohl die Administrator PIN als auch die User PIN auf der Karte gespeichert. Diese PINs werden bei der weiteren Nutzung der initialisierten Smartcard benötigt.

Das Menü „Smartcard Werkzeug“:



HINWEIS	
	Das Erstellen von Schlüsseln auf einer Smartcard ist im Abschnitt „Erstellen einer neuen Zertifikatsanforderung“ auf der Seite 33 beschrieben. Zum Speichern von X.509 Zertifikaten auf einer Smartcard wird das Menü „Zertifikate anzeigen / exportieren“ verwendet.

6.5.2. IPSEC Administration

Unter dem Menüpunkt „IPSEC Administration“ sind alle Werkzeuge zur Verwaltung von IPSEC Verbindungen zusammengefasst.

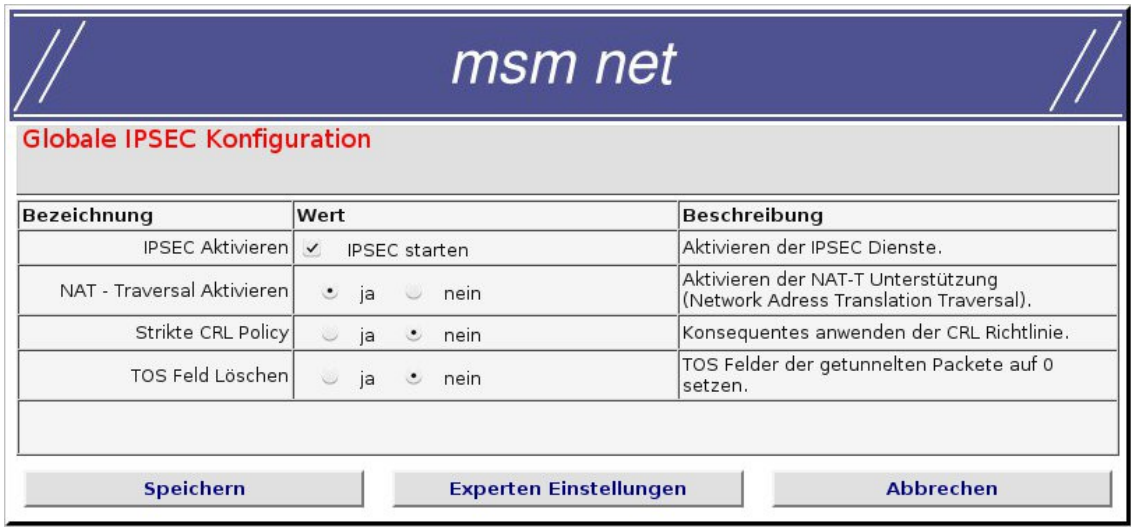
Das Menü stellt auf der linken Seite alle vorhandenen IPSEC Verbindungen dar. Wenn Sie eine Verbindung kopieren, bearbeiten oder löschen wollen, so müssen sie diese vorher markieren.

Auf der rechten Seite sind im Menü alle Werkzeuge zum Bearbeiten der Verbindungen angeordnet. Ist eine Aktion nicht möglich, wird eine Fehlermeldung angezeigt.

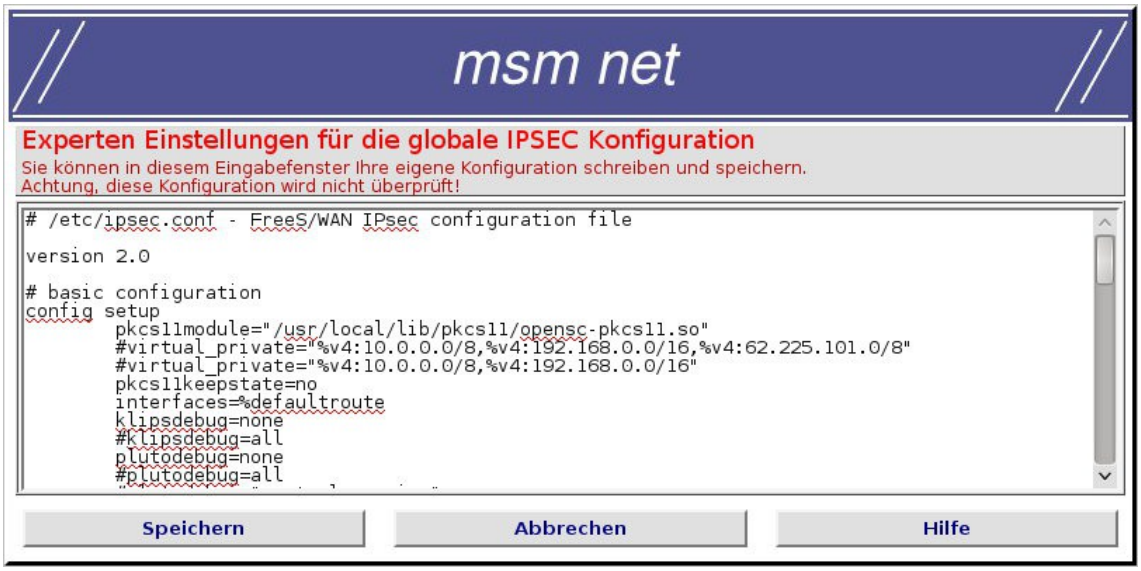
Das Menü "IPSEC VPN Verbindungen“:

Das Menü „Globale IPSEC Einstellungen“:

Gemeinsame Parameter, die für alle IPSEC Verbindungen gelten, werden in dem Menü „Globale IPSEC Einstellungen“ konfiguriert.



Das „Expert Einstellungen“ Menü für die globale IPSEC Konfiguration:

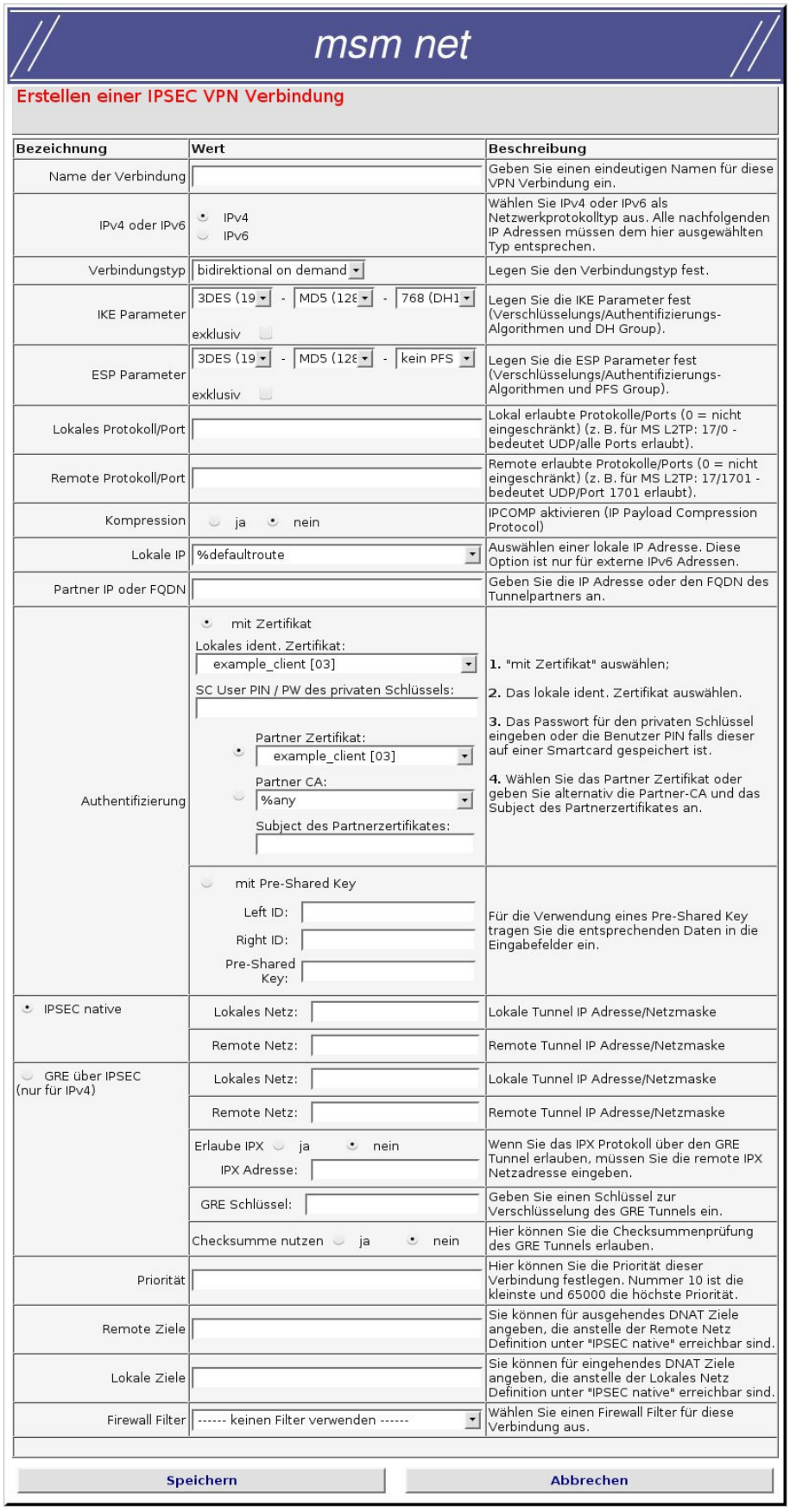


HINWEIS	
	Experten Einstellungen für die globale IPSEC Konfiguration: ➢ Die Konfigurationsdatei kann über das Menü direkt bearbeitet werden. ➢ Optionen für die es in der GUI keine Entsprechung gibt, können hier ebenfalls konfiguriert werden,. ➢ Unter „Hilfe“ ist eine detaillierte Hilfe zu den Optionen verfügbar. **Bitte beachten Sie, falsche oder inkorrekte Optionen können zu Funktionsstörungen des IPSEC führen !**

Anlegen einer neuen Verbindung

Klicken Sie auf die Schaltfläche „Anlegen einer neuen Verbindung“, um das Konfigurationsmenü zu öffnen.

Das Menü „Neue Verbindung anlegen“:



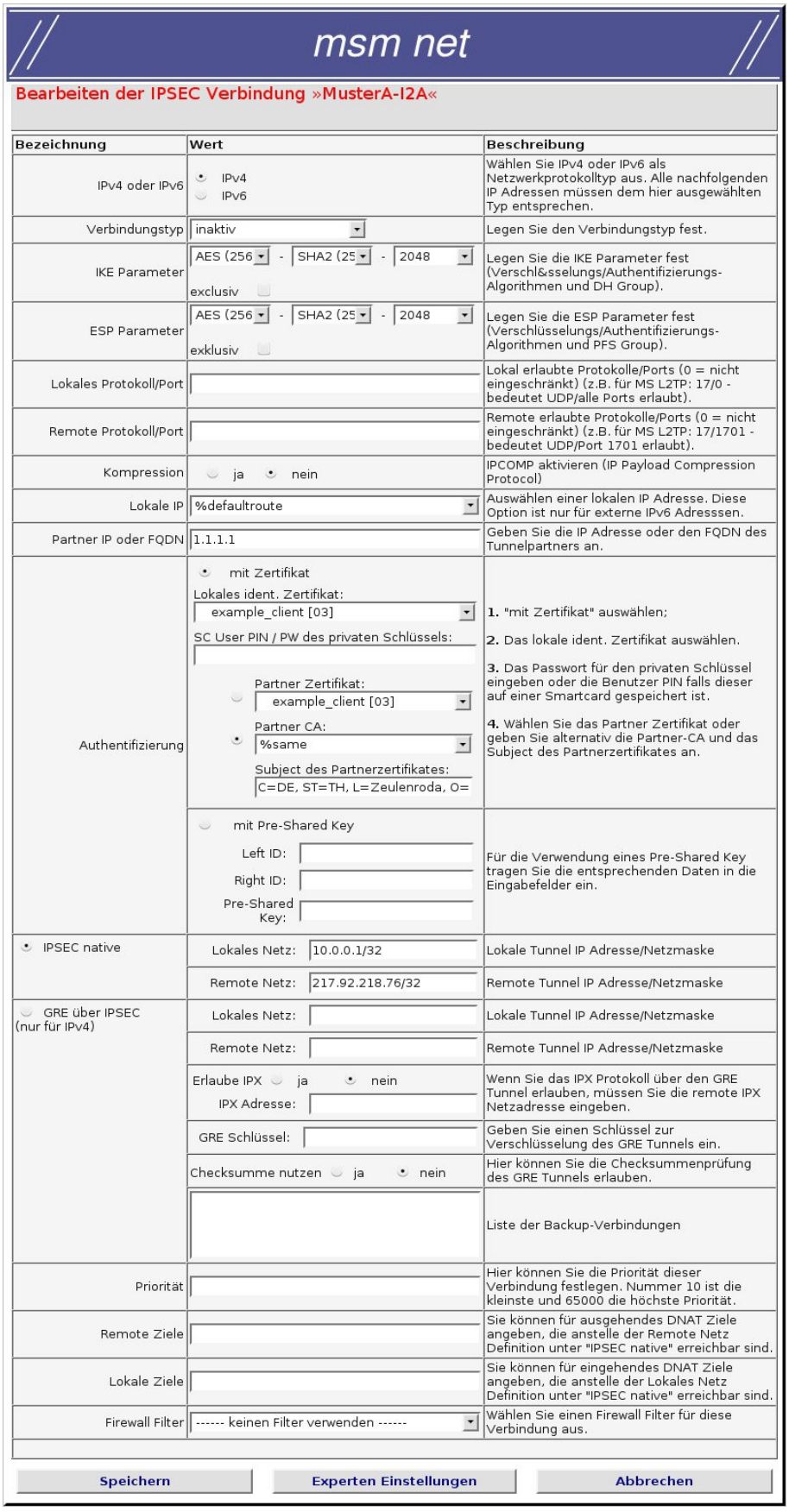
msm net

Erstellen einer IPSEC VPN Verbindung

Bezeichnung	Wert	Beschreibung
Name der Verbindung		Geben Sie einen eindeutigen Namen für diese VPN Verbindung ein.
IPv4 oder IPv6	IPv4 / IPv6	Wählen Sie IPv4 oder IPv6 als Netzwerkprotokolltyp aus. Alle nachfolgenden IP Adressen müssen dem hier ausgewählten Typ entsprechen.
Verbindungstyp	bidirektional on demand	Legen Sie den Verbindungstyp fest.
IKE Parameter	3DES (19 - MD5 (128 - 768 (DH1 exklusiv	Legen Sie die IKE Parameter fest (Verschlüsselungs/Authentifizierungs-Algorithmen und DH Group).
ESP Parameter	3DES (19 - MD5 (128 - kein PFS exklusiv	Legen Sie die ESP Parameter fest (Verschlüsselungs/Authentifizierungs-Algorithmen und PFS Group).
Lokales Protokoll/Port		Lokal erlaubte Protokolle/Ports (0 = nicht eingeschränkt) (z. B. für MS L2TP: 17/0 - bedeutet UDP/alle Ports erlaubt).
Remote Protokoll/Port		Remote erlaubte Protokolle/Ports (0 = nicht eingeschränkt) (z. B. für MS L2TP: 17/1701 - bedeutet UDP/Port 1701 erlaubt).
Kompression	ja / nein	IPCOMP aktivieren (IP Payload Compression Protocol)
Lokale IP	%defaultroute	Auswählen einer lokale IP Adresse. Diese Option ist nur für externe IPv6 Adressen.
Partner IP oder FQDN		Geben Sie die IP Adresse oder den FQDN des Tunnelpartners an.
Authentifizierung	mit Zertifikat Lokales ident. Zertifikat: example_client [03] SC User PIN / PW des privaten Schlüssels: Partner Zertifikat: example_client [03] Partner CA: %any Subject des Partnerzertifikates:	**1.** "mit Zertifikat" auswählen; **2.** Das lokale ident. Zertifikat auswählen. **3.** Das Passwort für den privaten Schlüssel eingeben oder die Benutzer PIN falls dieser auf einer Smartcard gespeichert ist. **4.** Wählen Sie das Partner Zertifikat oder geben Sie alternativ die Partner-CA und das Subject des Partnerzertifikates an.
	mit Pre-Shared Key Left ID: Right ID: Pre-Shared Key:	Für die Verwendung eines Pre-Shared Key tragen Sie die entsprechenden Daten in die Eingabefelder ein.
IPSEC native	Lokales Netz:	Lokale Tunnel IP Adresse/Netzmaske
	Remote Netz:	Remote Tunnel IP Adresse/Netzmaske
GRE über IPSEC (nur für IPv4)	Lokales Netz:	Lokale Tunnel IP Adresse/Netzmaske
	Remote Netz:	Remote Tunnel IP Adresse/Netzmaske
	Erlaube IPX ja / nein IPX Adresse:	Wenn Sie das IPX Protokoll über den GRE Tunnel erlauben, müssen Sie die remote IPX Netzadresse eingeben.
	GRE Schlüssel:	Geben Sie einen Schlüssel zur Verschlüsselung des GRE Tunnels ein.
	Checksumme nutzen ja / nein	Hier können Sie die Checksummenprüfung des GRE Tunnels erlauben.
Priorität		Hier können Sie die Priorität dieser Verbindung festlegen. Nummer 10 ist die kleinste und 65000 die höchste Priorität.
Remote Ziele		Sie können für ausgehendes DNAT Ziele angeben, die anstelle der Remote Netz Definition unter "IPSEC native" erreichbar sind.
Lokale Ziele		Sie können für eingehendes DNAT Ziele angeben, die anstelle der Lokales Netz Definition unter "IPSEC native" erreichbar sind.
Firewall Filter	------ keinen Filter verwenden ------	Wählen Sie einen Firewall Filter für diese Verbindung aus.

Speichern | Abbrechen

Das Menü „Verbindung bearbeiten“:


msm net
Bearbeiten der IPSEC Verbindung »MusterA-I2A«
Bezeichnung
Wert
Beschreibung
IPv4 oder IPv6
IPv4
IPv6
Wählen Sie IPv4 oder IPv6 als Netzwerkprotokolltyp aus. Alle nachfolgenden IP Adressen müssen dem hier ausgewählten Typ entsprechen.
Verbindungstyp
inaktiv
Legen Sie den Verbindungstyp fest.
IKE Parameter
AES (256 - SHA2 (25 - 2048
exclusiv
Legen Sie die IKE Parameter fest (Verschl&sselungs/Authentifizierungs-Algorithmen und DH Group).
ESP Parameter
AES (256 - SHA2 (25 - 2048
exklusiv
Legen Sie die ESP Parameter fest (Verschlüsselungs/Authentifizierungs-Algorithmen und PFS Group).
Lokales Protokoll/Port
Lokal erlaubte Protokolle/Ports (0 = nicht eingeschränkt) (z.B. für MS L2TP: 17/0 - bedeutet UDP/alle Ports erlaubt).
Remote Protokoll/Port
Remote erlaubte Protokolle/Ports (0 = nicht eingeschränkt) (z.B. für MS L2TP: 17/1701 - bedeutet UDP/Port 1701 erlaubt).
Kompression
ja
nein
IPCOMP aktivieren (IP Payload Compression Protocol)
Lokale IP
%defaultroute
Auswählen einer lokalen IP Adresse. Diese Option ist nur für externe IPv6 Adresssen.
Partner IP oder FQDN
1.1.1.1
Geben Sie die IP Adresse oder den FQDN des Tunnelpartners an.
Authentifizierung
mit Zertifikat
Lokales ident. Zertifikat:
example_client [03]
SC User PIN / PW des privaten Schlüssels:
Partner Zertifikat:
example_client [03]
Partner CA:
%same
Subject des Partnerzertifikates:
C=DE, ST=TH, L=Zeulenroda, O=
1. "mit Zertifikat" auswählen;
2. Das lokale ident. Zertifikat auswählen.
3. Das Passwort für den privaten Schlüssel eingeben oder die Benutzer PIN falls dieser auf einer Smartcard gespeichert ist.
4. Wählen Sie das Partner Zertifikat oder geben Sie alternativ die Partner-CA und das Subject des Partnerzertifikates an.
mit Pre-Shared Key
Left ID:
Right ID:
Pre-Shared Key:
Für die Verwendung eines Pre-Shared Key tragen Sie die entsprechenden Daten in die Eingabefelder ein.
IPSEC native
Lokales Netz:
10.0.0.1/32
Lokale Tunnel IP Adresse/Netzmaske
Remote Netz:
217.92.218.76/32
Remote Tunnel IP Adresse/Netzmaske
GRE über IPSEC (nur für IPv4)
Lokales Netz:
Lokale Tunnel IP Adresse/Netzmaske
Remote Netz:
Remote Tunnel IP Adresse/Netzmaske
Erlaube IPX
ja
nein
IPX Adresse:
Wenn Sie das IPX Protokoll über den GRE Tunnel erlauben, müssen Sie die remote IPX Netzadresse eingeben.
GRE Schlüssel:
Geben Sie einen Schlüssel zur Verschlüsselung des GRE Tunnels ein.
Checksumme nutzen
ja
nein
Hier können Sie die Checksummenprüfung des GRE Tunnels erlauben.
Liste der Backup-Verbindungen
Priorität
Hier können Sie die Priorität dieser Verbindung festlegen. Nummer 10 ist die kleinste und 65000 die höchste Priorität.
Remote Ziele
Sie können für ausgehendes DNAT Ziele angeben, die anstelle der Remote Netz Definition unter "IPSEC native" erreichbar sind.
Lokale Ziele
Sie können für eingehendes DNAT Ziele angeben, die anstelle der Lokales Netz Definition unter "IPSEC native" erreichbar sind.
Firewall Filter
------ keinen Filter verwenden ------
Wählen Sie einen Firewall Filter für diese Verbindung aus.
Speichern
Experten Einstellungen
Abbrechen

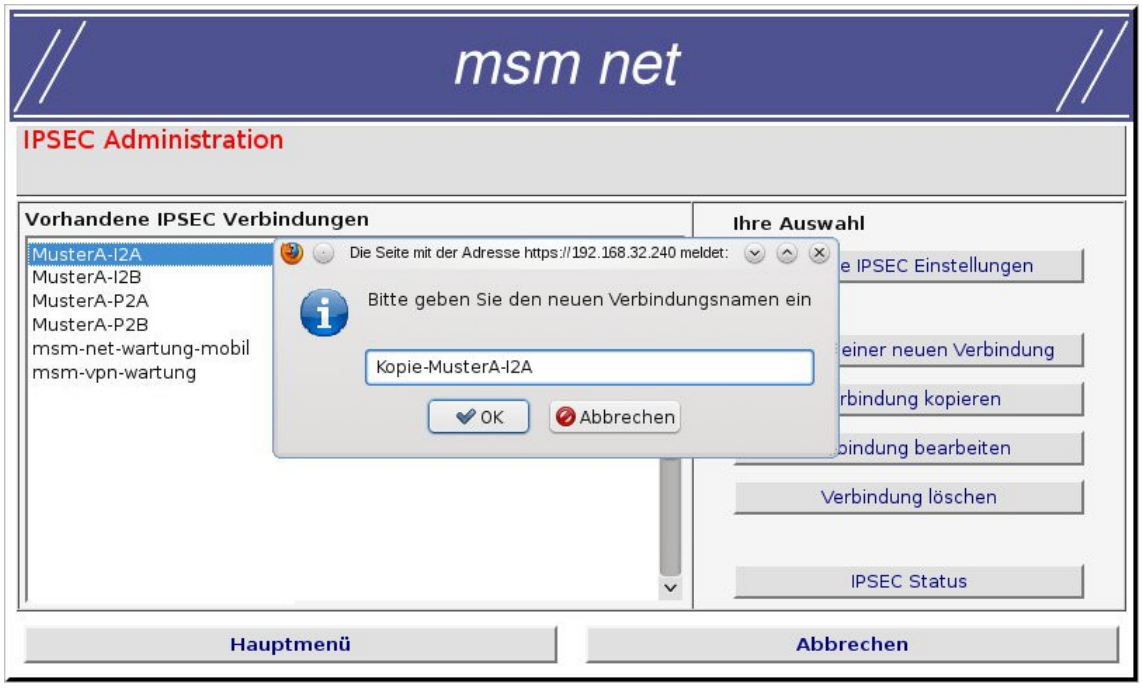
Das Menü „Experten Einstellungen“ einer IPSEC Verbindung:

HINWEIS	
	Das Menü „Experten Einstellungen“ einer VPN Verbindung: ➢ Diese Option steht beim Anlegen einer Verbindung noch nicht zur Verfügung. ➢ Kann über das Menü „Verbindung bearbeiten“ aufgerufen werde **Bitte beachten Sie, falsche oder inkorrekte Optionen können zu Funktionsstörungen des IPSEC führen!**

Kopieren einer Verbindung

Wenn mehrere Verbindungen mit ähnlichen Parametern konfiguriert werden sollen, empfiehlt es sich eine bestehende Verbindung zu kopieren. Während des Kopiervorganges werden Sie zur Eingabe eines neuen Verbindungsnamens aufgefordert, alle anderen Einstellungen werden übernommen und die Verbindung als inaktiv angelegt. Danach öffnet sich das Konfigurationsfenster der kopierten Verbindung. Wenn Sie alle notwendigen Anpassungen vorgenommen haben, kann die Verbindung mit einem Klick auf die Schaltfläche „Speichern“ gesichert werden.

Das Menü „Verbindung kopieren“:



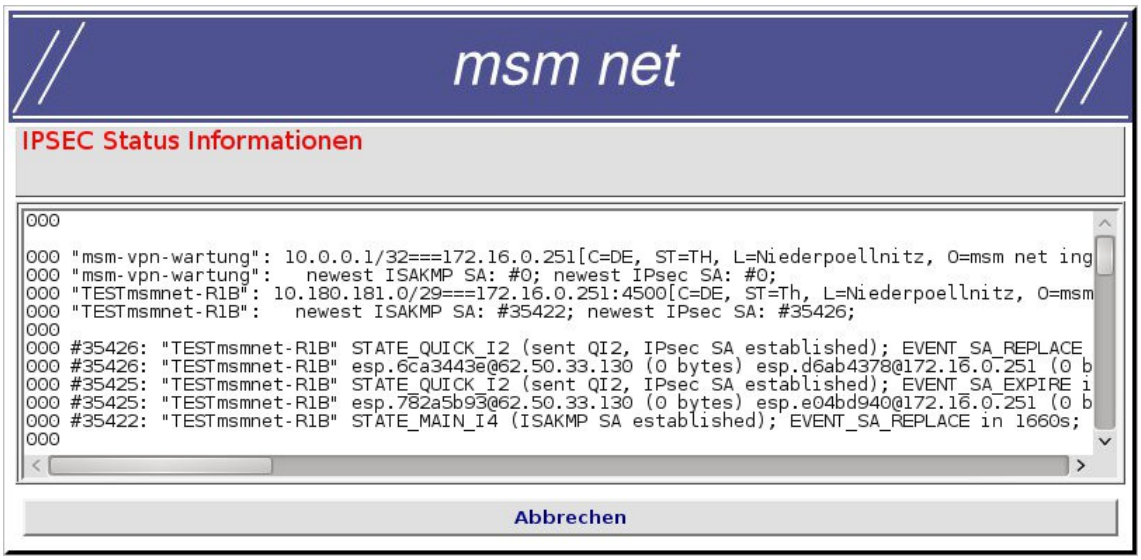
HINWEIS	
	Parameter von VPN Verbindungen: ➢ Haben verschieden Verbindungen identische Parameter, kann gleichzeitig immer nur eine Verbindung aktiv sein. Dies ist insbesondere bei HA Verbindungen zu beachten. Die Steuerung erfolgt dort mit dem Parameter „Priorität“.

Die Warnmeldung „Löschen einer Verbindung“:

msm net
Löschen der IPSEC VPN Verbindung »MusterA-I2A«
!! Warnung !!
Mit dem Löschen der IPSEC VPN Verbindung werden ebenfalls alle zugehörigen Daten gelöscht.
Die Löschung erfolgt permanent.
Wenn Sie sicher sind, dann klicken Sie auf "Löschen".
Löschen
Abbrechen

Hinweis	
	➢ Bevor eine Verbindung gelöscht werden kann, muss sie erst deaktiviert werden.

Das Menü „IPSEC Status“:


msm net
IPSEC Status Informationen
000
000 "msm-vpn-wartung": 10.0.0.1/32===172.16.0.251[C=DE, ST=TH, L=Niederpoellnitz, O=msm net ing
000 "msm-vpn-wartung": newest ISAKMP SA: #0; newest IPsec SA: #0;
000 "TESTmsmnet-R1B": 10.180.181.0/29===172.16.0.251:4500[C=DE, ST=Th, L=Niederpoellnitz, O=msm
000 "TESTmsmnet-R1B": newest ISAKMP SA: #35422; newest IPsec SA: #35426;
000
000 #35426: "TESTmsmnet-R1B" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE
000 #35426: "TESTmsmnet-R1B" esp.6ca3443e@62.50.33.130 (0 bytes) esp.d6ab4378@172.16.0.251 (0 b
000 #35425: "TESTmsmnet-R1B" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_EXPIRE i
000 #35425: "TESTmsmnet-R1B" esp.782a5b93@62.50.33.130 (0 bytes) esp.e04bd940@172.16.0.251 (0 b
000 #35422: "TESTmsmnet-R1B" STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 1660s;
000
Abbrechen

6.5.3. L2TP Administration

Zum Herstellen von VPN Verbindungen über das „Layer 2 Transport Protocol“ ist in unsere VPN Appliances ein L2TP Server integriert. Alle auf die VPN Appliance bezogenen Einstellungen können in dem nachfolgenden Menü vorgenommen werden. Die Benutzerverwaltung kann lokal, unter der „Benutzerverwaltung“ im Hauptmenü oder über einen RADIUS-Server erfolgen.

Da L2TP nur in Verbindung mit IPSEC unterstützt wird, erfolgt die Konfiguration einer eingehenden IPSEC Verbindung zur Verwendung von L2TP im Menü „IPSEC VPN Verbindungen“. Die Konfiguration erfolgt in den Eigenschaften einer Verbindung unter den folgenden Abschnitten:

- „Lokales Protokoll / Port“: z.B.: 17/1701
- „Remote Protokoll / Port“ z.B.: 17/1701
- „Partner IP oder FQDN“ z.B.: %any für Zugriff von jeder IP Adresse
- „Authentifizierung“: z.B.: mit Zertifikaten
- „IPSEC native Lokales Netz“: Kein Eintrag!
- „IPSEC native Remote Netz“: z.B.: vhost:%all!
- „Firewall Filter“: Eine Regel für den IPSEC Teil der Verbindung; benutzerspezifische Firewall Filter werden aktiviert, sobald die L2TP Verbindung nach erfolgter Benutzerauthentifizierung etabliert wird.

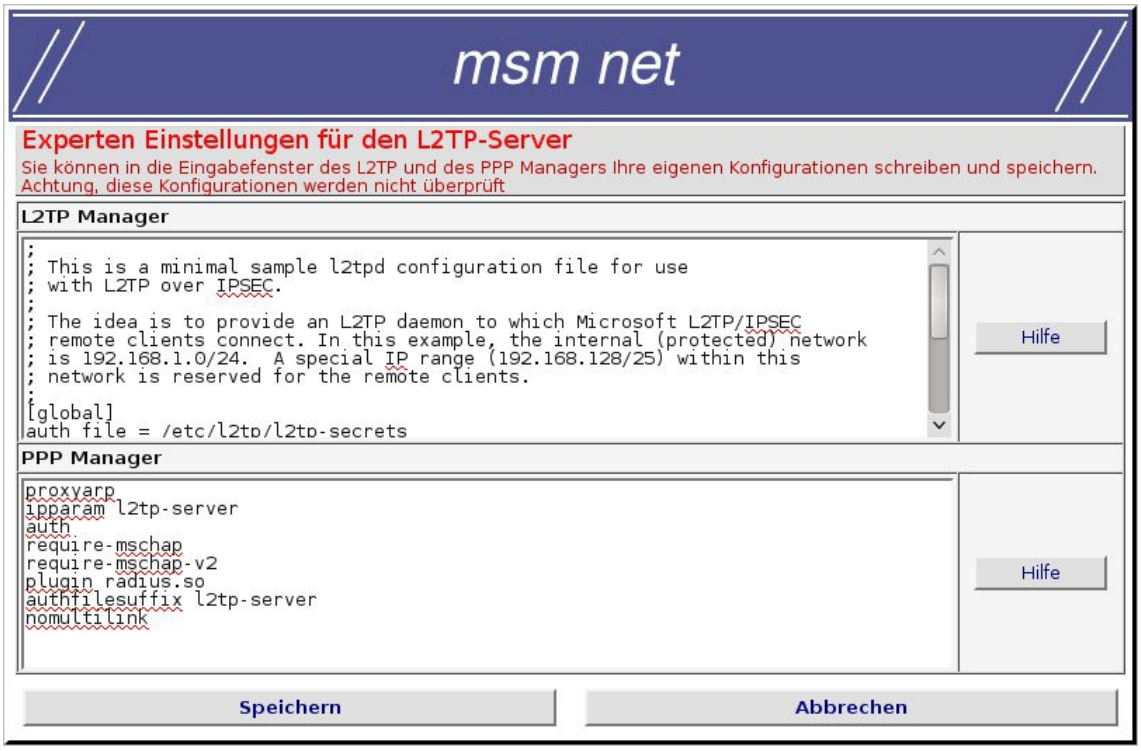
Das Menü „L2TP Server Einstellungen“:

msm net
L2TP Server Einstellungen
L2TP Verbindungen arbeiten nur über IPSEC Tunnel.
Bezeichnung
Wert
Beschreibung
L2TP Server Aktivieren
L2TP Server starten
Aktivieren des L2TP Servers.
L2TP Server IP Adresse
192.168.100.1
Geben Sie für den L2TP Server eine IP Adresse ein. Diese darf nicht identisch mit der IP Adresse des internen Interface sein.
Client IP Adressbereich
192.168.100.2-192.168.100.254
Ein Pool von IP Adressen der vom L2TP Server an Clients verteilt wird.
autom. Trennung nach
nie
Hier legen Sie fest, nach welcher Leerlaufzeit die Verbindung getrennt werden soll.
Authentifizierung
Lokale Benutzerauthentifizierung
Remote via RADIUS
Wählen Sie zwischen lokaler oder remote Authentifizierung via RADIUS Server (siehe Menü Service -> RADIUS Client).
Authentifizierungmethode
CHAP
CHAP-MS-V1
CHAP-MS-V2
PAP
Hier können Sie die erlaubten Authentifizierungsmethoden auswählen.
Speichern
Experten Einstellungen
Abbrechen

Experten Einstellungen für den L2TP Server

Bestehen darüber hinaus weitergehende Konfigurationsanforderungen, können diese über das Menü „Experten Einstellungen“ direkt in den Konfigurationsdateien des L2TP Servers erfolgen. Dort ist auch eine ausführliche Online-Hilfe über alle Konfigurationsparameter vorhanden.

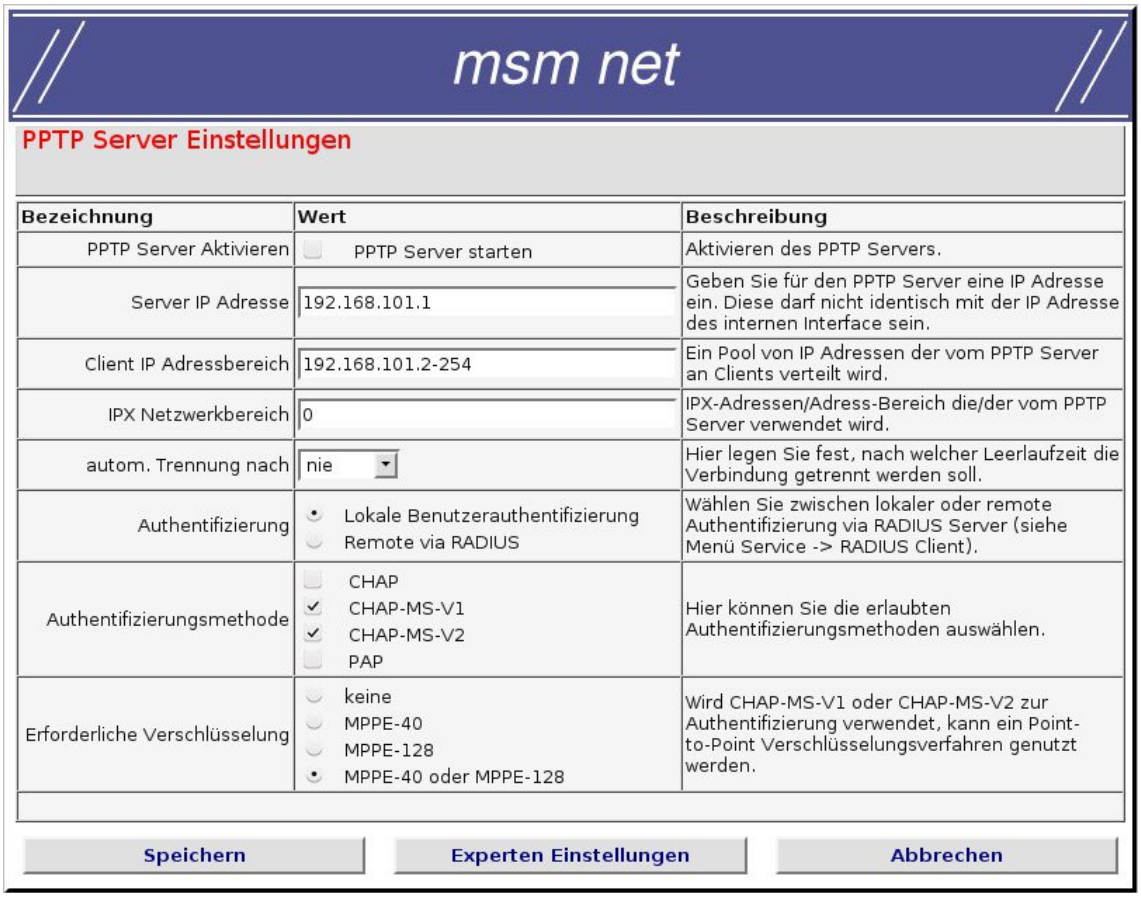
Das „Experten Menü“ für den L2TP-Server:


msm net
Experten Einstellungen für den L2TP-Server
Sie können in die Eingabefenster des L2TP und des PPP Managers Ihre eigenen Konfigurationen schreiben und speichern.
Achtung, diese Konfigurationen werden nicht überprüft
L2TP Manager
;
; This is a minimal sample l2tpd configuration file for use
; with L2TP over IPSEC.
;
; The idea is to provide an L2TP daemon to which Microsoft L2TP/IPSEC
; remote clients connect. In this example, the internal (protected) network
; is 192.168.1.0/24. A special IP range (192.168.128/25) within this
; network is reserved for the remote clients.
;
[global]
auth file = /etc/l2tp/l2tp-secrets
Hilfe
PPP Manager
proxyarp
ipparam l2tp-server
auth
require-mschap
require-mschap-v2
plugin radius.so
authfilesuffix l2tp-server
nomultilink
Hilfe
Speichern
Abbrechen

6.5.4. PPTP Administration

Zum Herstellen von VPN Verbindungen über das „Point-to-Point Tunneling Protocol“ ist in unsere VPN Appliance ein PPTP Server integriert. Alle für die Verbindung relevanten Einstellungen können in diesem Menü vorgenommen werden. Die Benutzerverwaltung kann über einen RADIUS-Server oder lokal unter der „Benutzerverwaltung“ im Hauptmenü erfolgen. Dort erfolgt auch die Einstellung ob ein Benutzer Verbindungen zum PPTP Server aufbauen darf.

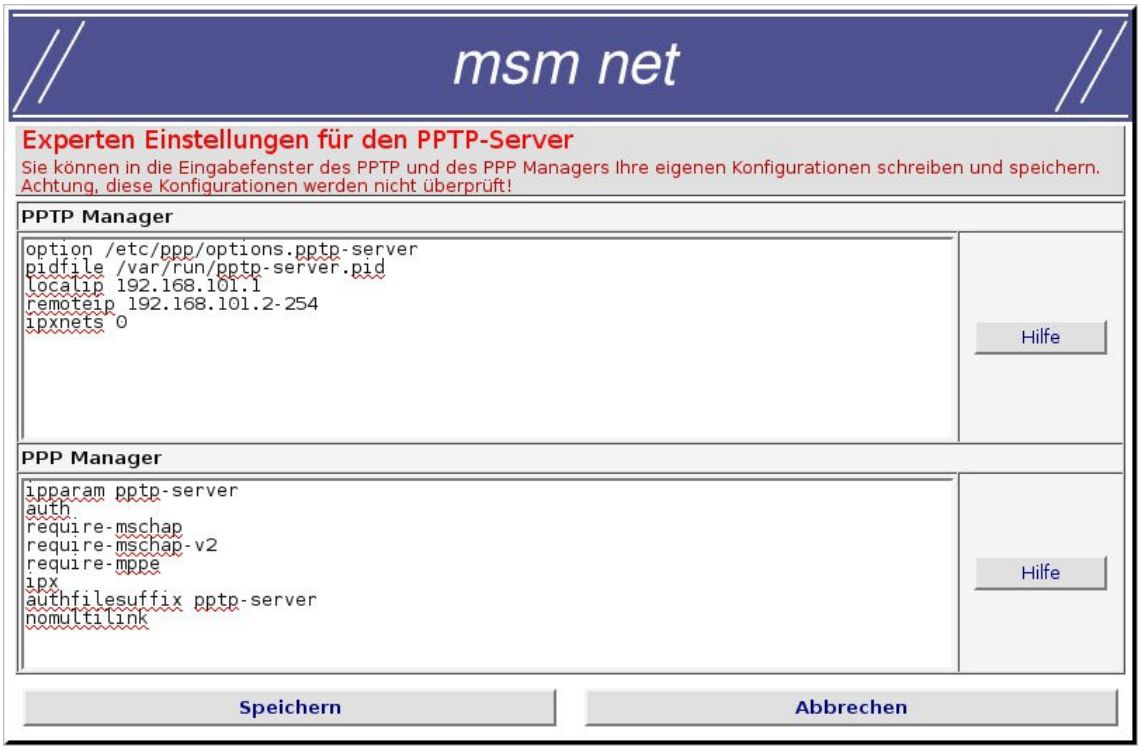
Das Menü „PPTP VPN Verbindungen“:



Experten Einstellungen für den PPTP Server

Bestehen darüber hinaus weitergehende Konfigurationsanforderungen, können diese über das Menü „Experten Einstellungen“ direkt in den Konfigurationsdateien des PPTP Servers erfolgen. Dort ist auch eine ausführliche Online-Hilfe über alle Konfigurationsparameter vorhanden.

Das Menü „Experten Einstellungen“ für den PPTP-Server:



6.6. Firewall Einstellungen

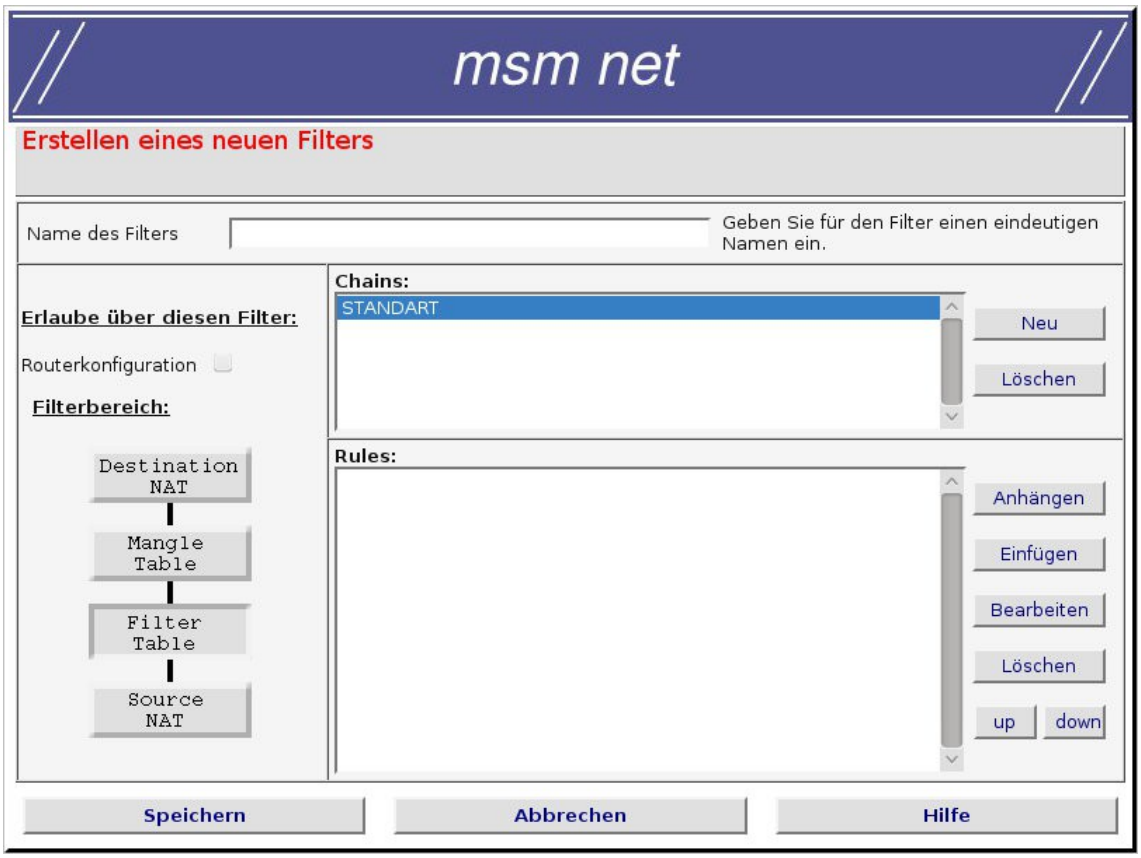
Die unter dem Menü Firewall Einstellungen verfügbaren Werkzeuge, ermöglichen mittels grafischer Oberflächen eine komfortable Verwaltung des auf die VPN Appliance angepassten IPTABLES Firewallpaketes.

Der vorkonfigurierte Filter „welcome“ ermöglicht den Zugriff auf das interne Interface der VPN Appliance. Wird er einem bestimmten Benutzer zugewiesen, ist es dem Benutzer – während er über eine VPN Verbindung mit der Appliance verbunden ist – gestattet auf die Konfigurationsoberfläche der VPN Appliance zuzugreifen und erlaubte Einstellungen z.B.: sein Passwort zu ändern.

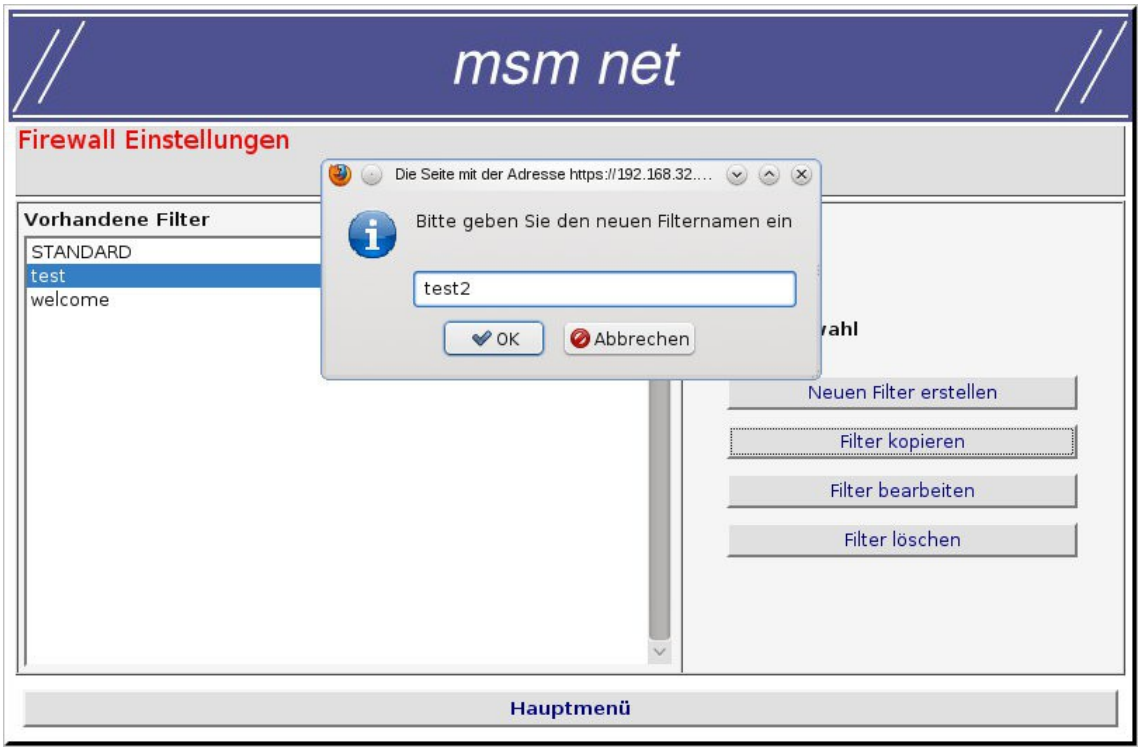
Alle verfügbaren Firewall Filter können sowohl einzelnen Benutzern als auch IPSEC Verbindungen zugeordnet werden. Eine Mehrfachzuordnung der Firewall Filter ist möglich.

Das Menü „Firewall Einstellungen“:

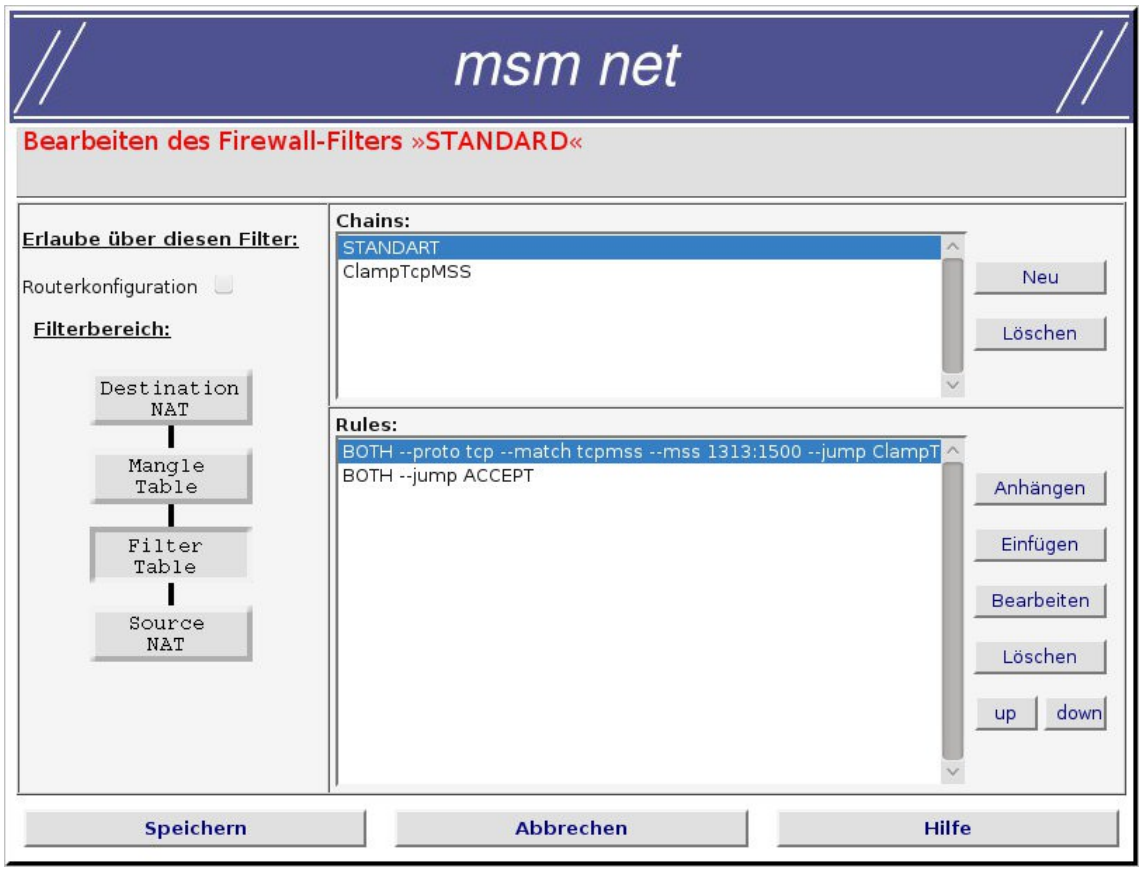
Das Menü „Neuen Filter erstellen”:



Das Menü „Filter Kopieren“:



Das Menü „Filter bearbeiten“:



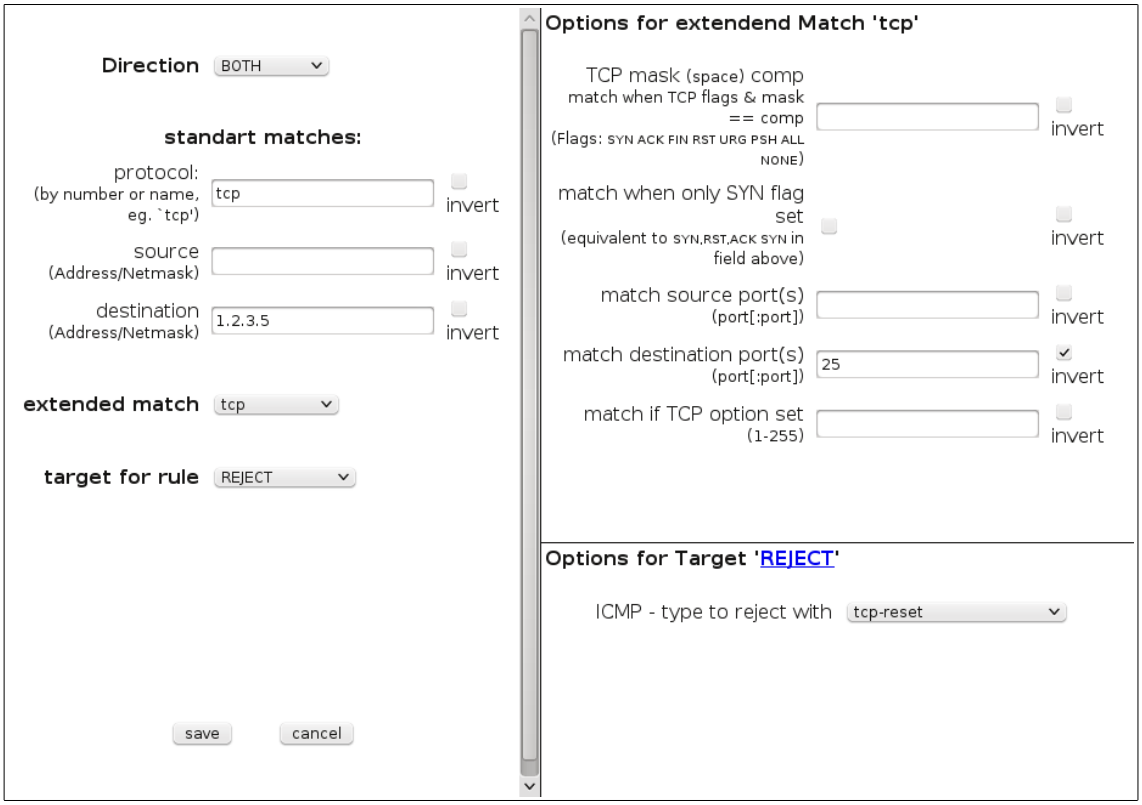
Das oben stehende Menü zeigt den Inhalt des Firewall Filters „STANDARD“. Die auf der linken Seite sichtbaren Filterbereiche werden von oben nach unten abgearbeitet. In der Abbildung ist im rechten oberen Bereich die Chain „STANDART“ ausgewählt. Im darunterliegenden Bereich „Rules:“ werden die eigentlichen Regeln angezeigt. Es ist zu beachten, dass die Regeln sequentiell, von oben nach unten abgearbeitet werden. Die Einträge können mit den Schaltflächen ganz rechts manipuliert werden. Die Änderungen werden sofort nach dem Speichern des Filters wirksam.

HINWEIS	
	Schaltfläche „Anhängen“: ➢ Eine neue Regel wird an letzter Stelle eingefügt. **Schaltfläche „Einfügen“:** ➢ Eine neue Regel wird oberhalb der markierten Regel eingefügt. **Schaltfläche „Bearbeiten“:** ➢ Die markierte Regel wird zum Bearbeiten geöffnet. **Schaltfläche „Löschen“:** ➢ Die markierte Regel wird gelöscht. **Schaltflächen „up“; „down“:** ➢ Die markierte Regel wird in die gewählte Richtung verschoben.

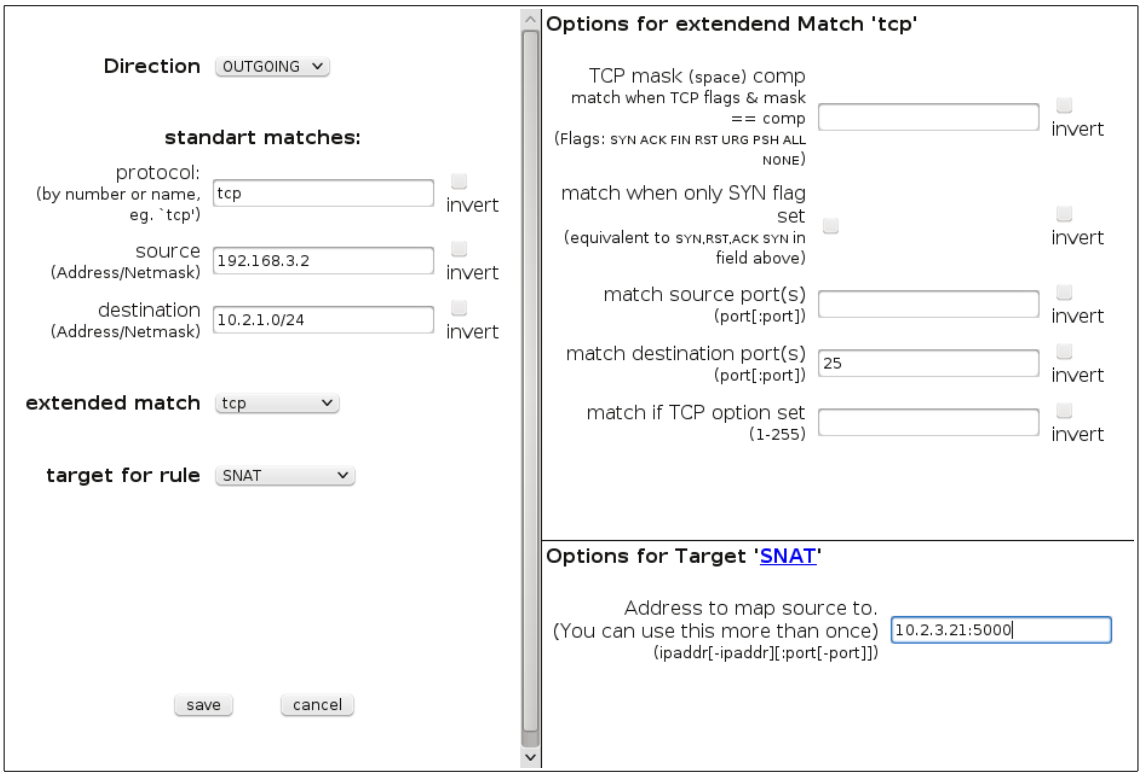
Wird eine Regel eingefügt oder bearbeitet, öffnet sich in einem neuen Browser-Fenster ein Bearbeitungsmenü.

Die Struktur des Bearbeitungsmenüs wird dynamisch an die ausgewählten Optionen angepasst. Daher sind die auf dieser Seite dargestellten Abbildungen lediglich als Beispiele zu sehen.

Das Bearbeitungsmenü einer Regel zum gezielten Abweisen von Traffic mit einer „tcp-reset" Meldung:


Direction BOTH
standart matches:
protocol: (by number or name, eg. `tcp') tcp invert
source (Address/Netmask) invert
destination (Address/Netmask) 1.2.3.5 invert
extended match tcp
target for rule REJECT
save
cancel
Options for extendend Match 'tcp'
TCP mask (space) comp match when TCP flags & mask == comp (Flags: SYN ACK FIN RST URG PSH ALL NONE) invert
match when only SYN flag set (equivalent to SYN,RST,ACK SYN in field above) invert
match source port(s) (port[:port]) invert
match destination port(s) (port[:port]) 25 invert
match if TCP option set (1-255) invert
Options for Target 'REJECT'
ICMP - type to reject with tcp-reset

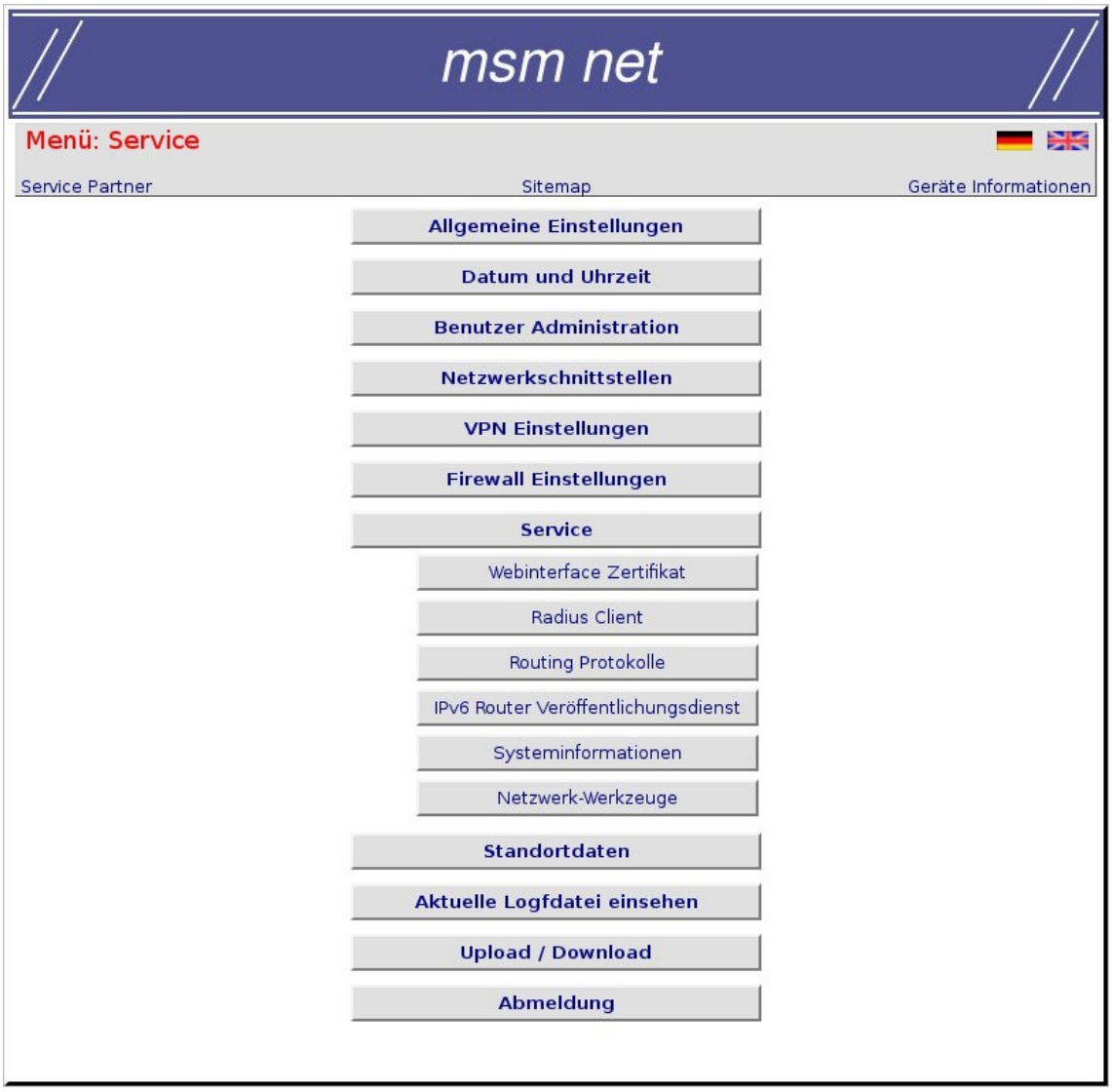
Das Bearbeitungsmenü für eine ausgehende Source NAT Regel:


Direction OUTGOING
standart matches:
protocol: (by number or name, eg. `tcp') tcp invert
source (Address/Netmask) 192.168.3.2 invert
destination (Address/Netmask) 10.2.1.0/24 invert
extended match tcp
target for rule SNAT
save
cancel
Options for extendend Match 'tcp'
TCP mask (space) comp match when TCP flags & mask == comp (Flags: SYN ACK FIN RST URG PSH ALL NONE) invert
match when only SYN flag set (equivalent to SYN,RST,ACK SYN in field above) invert
match source port(s) (port[:port]) invert
match destination port(s) (port[:port]) 25 invert
match if TCP option set (1-255) invert
Options for Target 'SNAT'
Address to map source to. (You can use this more than once) 10.2.3.21:5000
(ipaddr[-ipaddr][:port[-port]])

Die Warnmeldung „Filter löschen“:

msm net
Löschen des Filters »test«
!! Warnung !!
Stellen Sie vor dem Löschen sicher, dass der Firewall-Filter nicht mehr verwendet wird.
Das Löschen ist endgültig.
Fahren Sie fort, wenn Sie sicher sind.
Löschen
Abbrechen

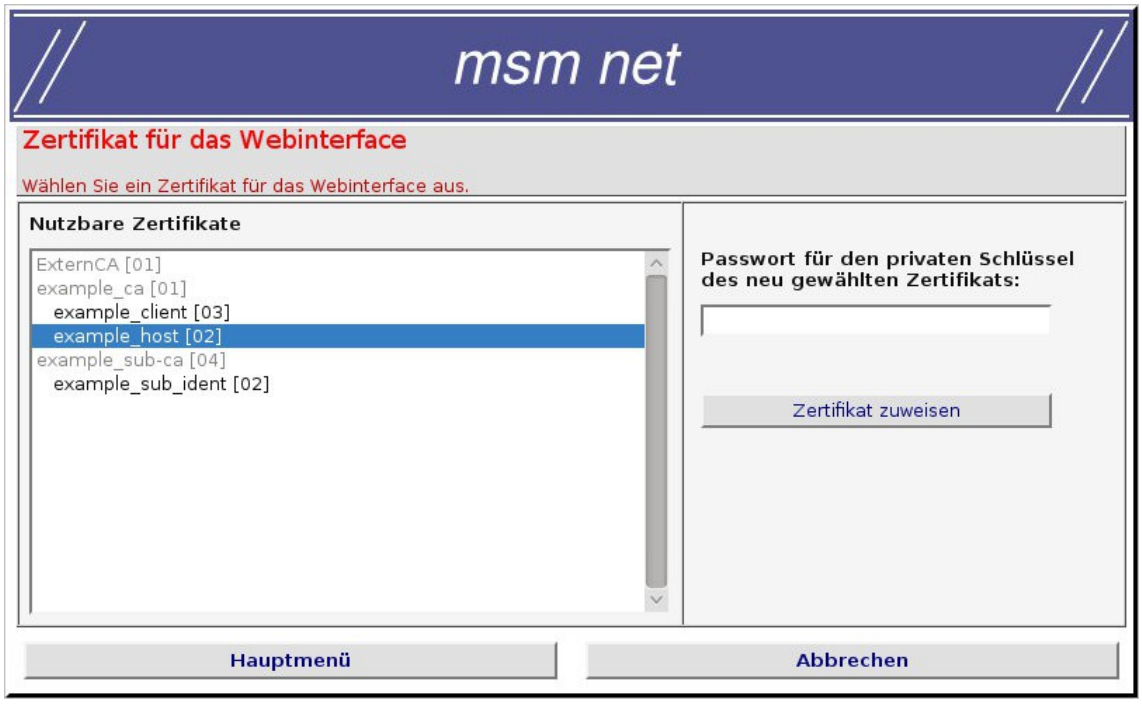
6.7. Das Service Menü



6.7.1. Zuweisen eines Zertifikates für das Webinterface

Mit diesem Menü kann für die Authentifizierung des integrierten Webservers ein Zertifikat zugewiesen werden.

Das Menü „Webinterface Zertifikat“:

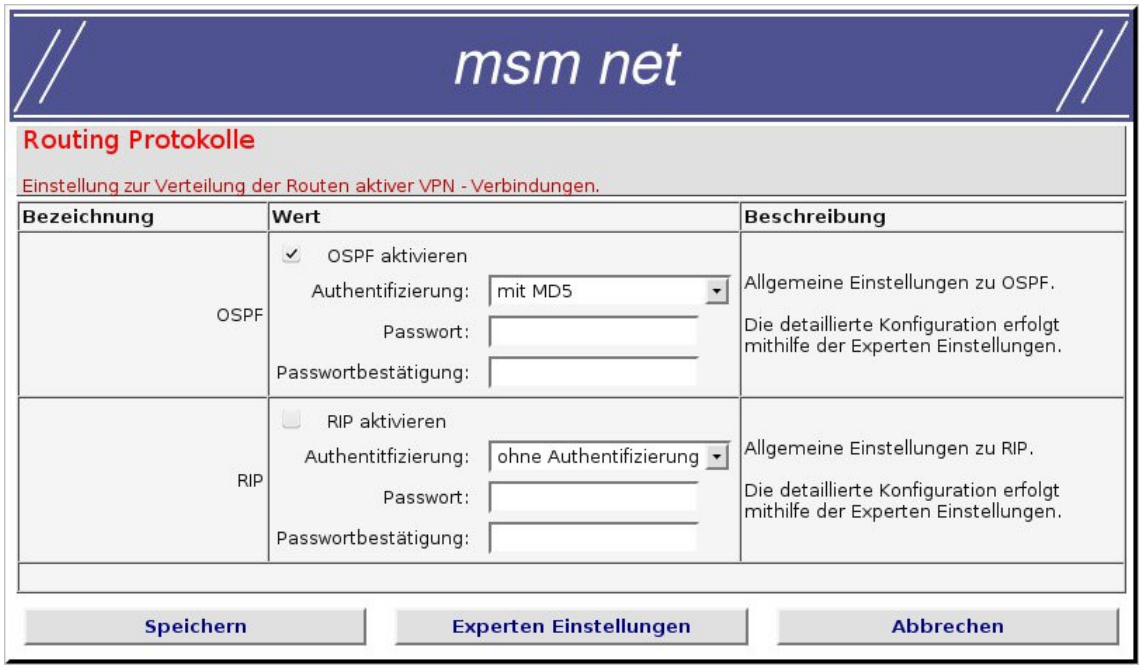


6.7.2. RADIUS-Client

6.7.3. Routing Protokoll Konfiguration

Werden zwei oder mehrere VPN Appliances als HA Cluster betrieben, sind diese über eine gemeinsame virtuelle IP-Adresse anzusprechen. Der Routing Daemon steuert, über welche VPN Appliance des HA Clusters Daten übertragen werden. Die Kommunikation der VPN Appliances wird durch gegenseitige Authentifizierung abgesichert.

Das Menü „Routing Protokolle“:

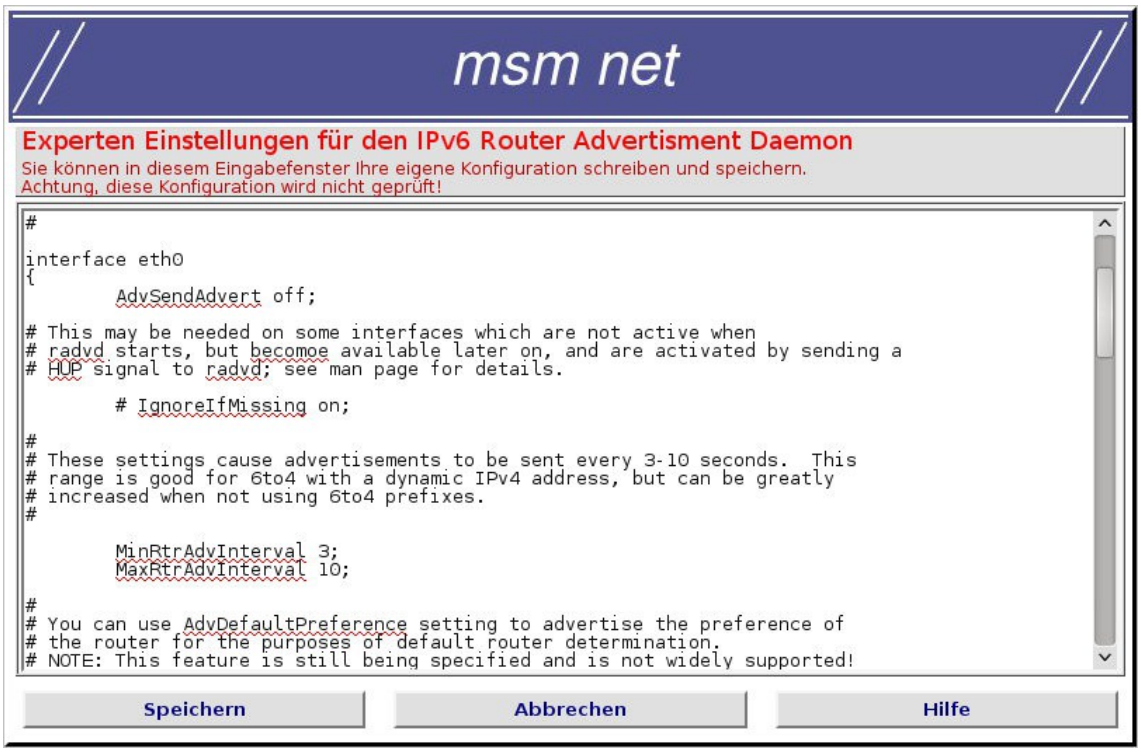


Das Menü „Experten Einstellungen“ für die Routing Protokoll Konfiguration:

6.7.4. Ipv6 Router Veröffentlichungsdienst

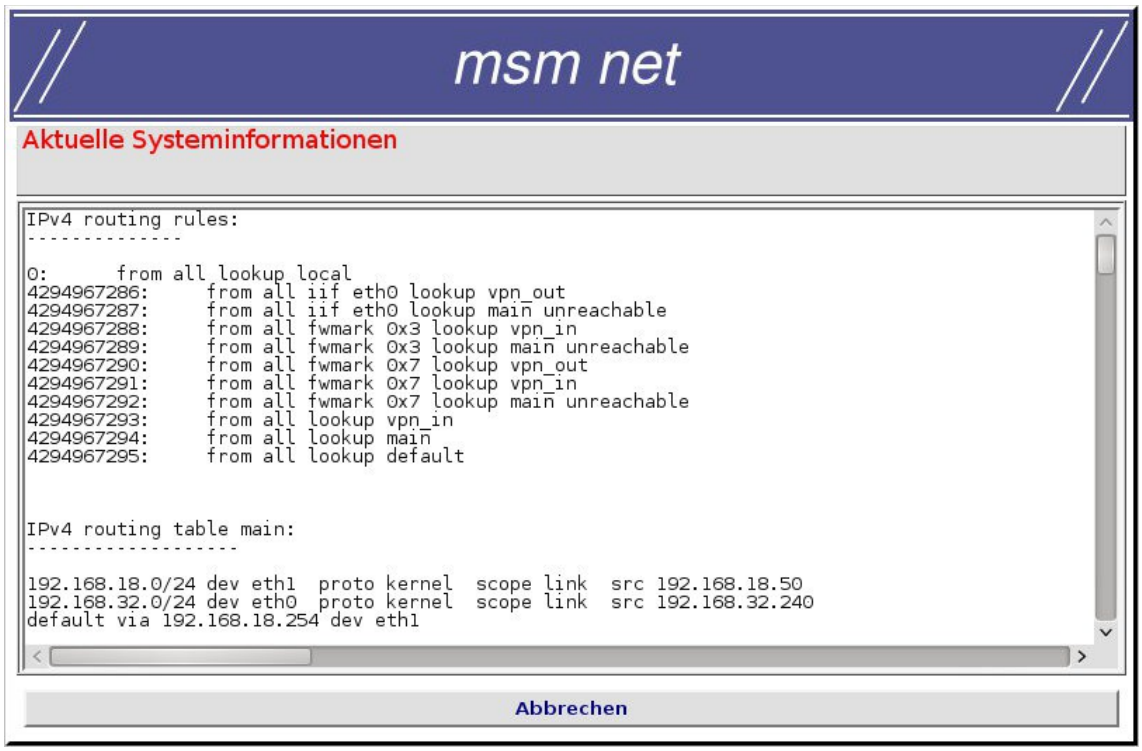
Soll die VPN Appliance IPv6 verwenden, können hier die Parameter direkt in der Konfigurationsdatei angepasst werden.

Das Menü „IPv6 Router Veröffentlichungsdienst“:


msm net
Experten Einstellungen für den IPv6 Router Advertisment Daemon
Sie können in diesem Eingabefenster Ihre eigene Konfiguration schreiben und speichern.
Achtung, diese Konfiguration wird nicht geprüft!
#
interface eth0
{
AdvSendAdvert off;
This may be needed on some interfaces which are not active when
radvd starts, but becomoe available later on, and are activated by sending a
HUP signal to radvd; see man page for details.
IgnoreIfMissing on;
#
These settings cause advertisements to be sent every 3-10 seconds. This
range is good for 6to4 with a dynamic IPv4 address, but can be greatly
increased when not using 6to4 prefixes.
#
MinRtrAdvInterval 3;
MaxRtrAdvInterval 10;
#
You can use AdvDefaultPreference setting to advertise the preference of
the router for the purposes of default router determination.
NOTE: This feature is still being specified and is not widely supported!
Speichern
Abbrechen
Hilfe

6.7.5. Systeminformationen

Das Menü „Systeminformationen“:


msm net
Aktuelle Systeminformationen
IPv4 routing rules:
0: from all lookup local
4294967286: from all iif eth0 lookup vpn_out
4294967287: from all iif eth0 lookup main unreachable
4294967288: from all fwmark 0x3 lookup vpn_in
4294967289: from all fwmark 0x3 lookup main unreachable
4294967290: from all fwmark 0x7 lookup vpn_out
4294967291: from all fwmark 0x7 lookup vpn_in
4294967292: from all fwmark 0x7 lookup main unreachable
4294967293: from all lookup vpn_in
4294967294: from all lookup main
4294967295: from all lookup default
IPv4 routing table main:
192.168.18.0/24 dev eth1 proto kernel scope link src 192.168.18.50
192.168.32.0/24 dev eth0 proto kernel scope link src 192.168.32.240
default via 192.168.18.254 dev eth1
Abbrechen

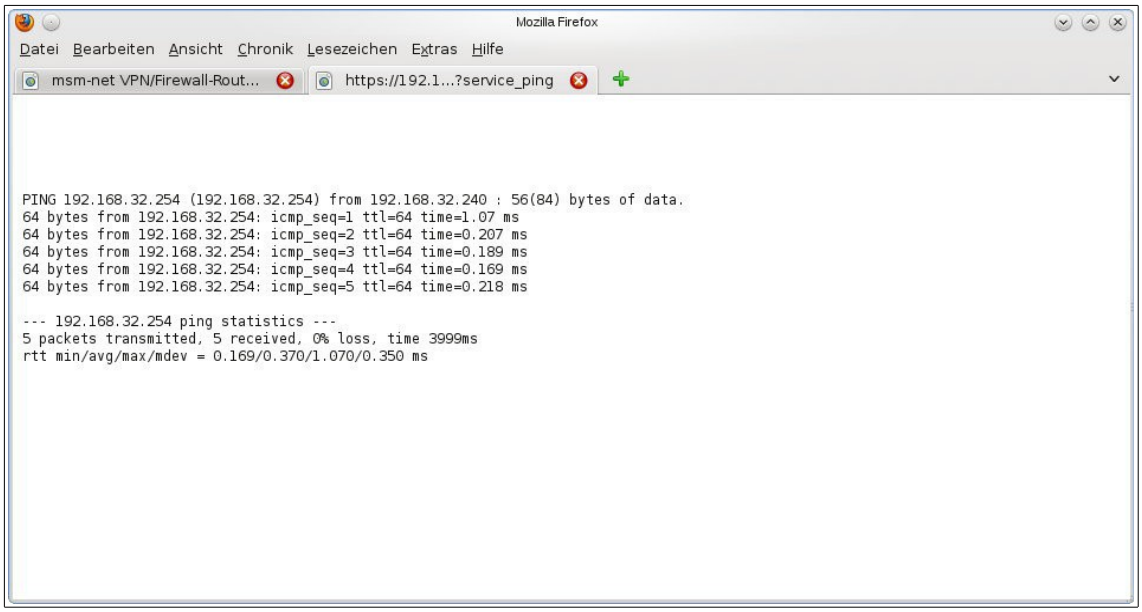
In den „Systeminformationen“ kann sich ein versierter Techniker über den aktuellen Zustand der VPN Appliance informieren. Bitte beachten Sie, der Listeninhalt entspricht dem aktuellen Systemzustand zum Zeitpunkt des Aufrufes.

6.7.6. Netzwerk-Werkzeuge

Die Werkzeuge „ICMP Echo Request“, „Network Dump“ und „Traceroute“ können über die Konfigurationsoberfläche direkt aus dem Menü „Netzwerk-Werkzeuge“ gestartet werden. In Abhängigkeit vom verwendeten Browser werden die Ergebnisse in einem neuen Fenster oder einem neuen Tab angezeigt.

Das Menü „Netzwerk-Werkzeuge“:

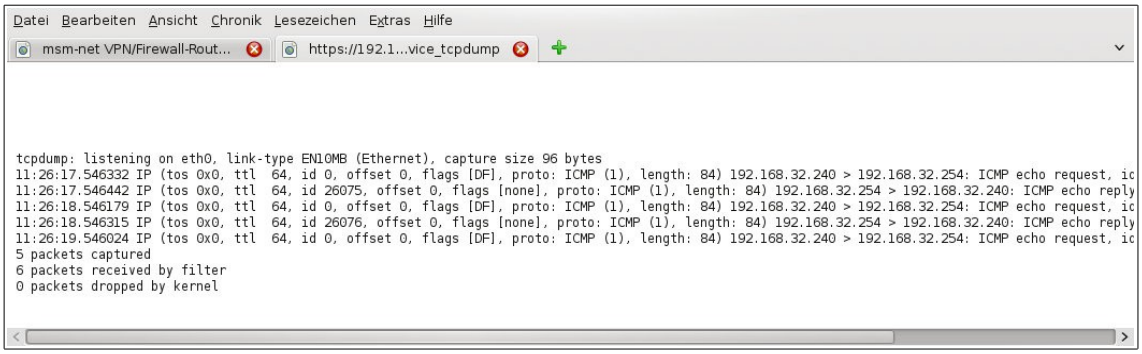
„ICMP Echo Request“:


Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
msm-net VPN/Firewall-Rout...
https://192.1...?service_ping
PING 192.168.32.254 (192.168.32.254) from 192.168.32.240 : 56(84) bytes of data.
64 bytes from 192.168.32.254: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.32.254: icmp_seq=2 ttl=64 time=0.207 ms
64 bytes from 192.168.32.254: icmp_seq=3 ttl=64 time=0.189 ms
64 bytes from 192.168.32.254: icmp_seq=4 ttl=64 time=0.169 ms
64 bytes from 192.168.32.254: icmp_seq=5 ttl=64 time=0.218 ms
--- 192.168.32.254 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 3999ms
rtt min/avg/max/mdev = 0.169/0.370/1.070/0.350 ms

HINWEIS	
	Das Ergebnis des „ICMP Echo Requests“ wird erst nach dem vollständigen Durchlaufen des Befehls angezeigt. Eine kleinere Anzahl von Pakete führt daher rascher zum Ergebnis. Die Ergebnisfenster oder Tabs können einfach geschlossen werden.

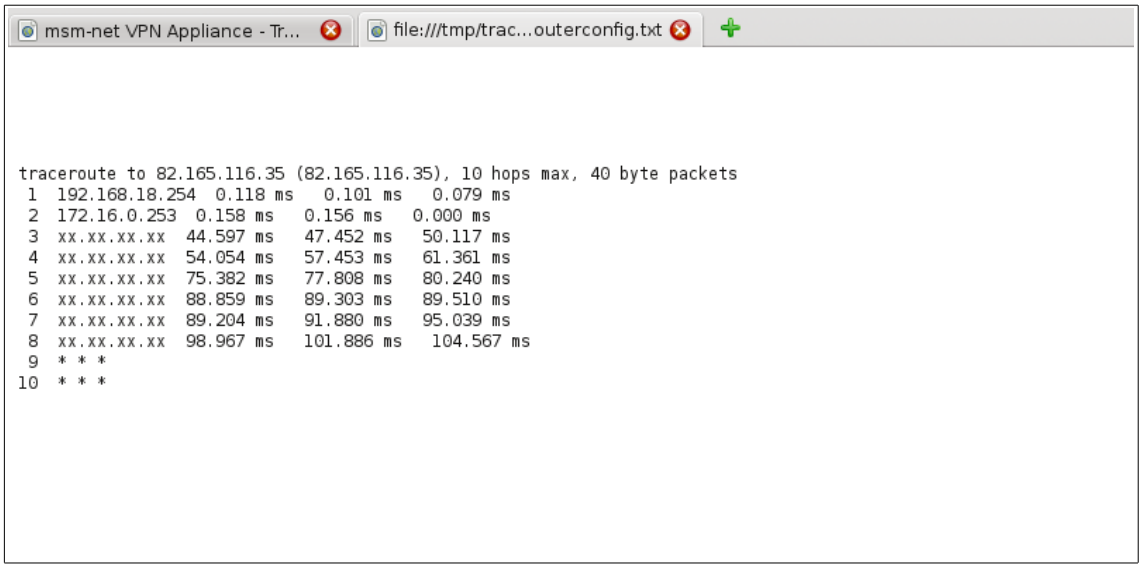
„Netzwerk Dump“:

msm net
Netzwerk Dump
Wählen Sie die Optionen für das Erstellen des Netzwerk Dumps und betätigen Sie "START DUMP"!
Nach Ausführung des Befehls wird das Ergebnis in einem neuen Browserfenster oder TAB angezeigt.
Bezeichnung
Wert
Beschreibung
Netzwerkschnittstelle
IF-EXTERN
Wählen Sie die Netzwerkschnittstelle aus. Nur die gwählte Schnittstelle wird für den Dump genutzt.
IP Adresse
Geben Sie für den Ausgabefilter eine IP Adresse ein (optional).
Protokoll
ANY
Ein IP Protokoll für den Ausgabefilter wählen. Der Term ANY bedeutet keine Filterung.
Paketanzahl
1
Wählen Sie die Anzahl der zu verarbeitenden Datenpakete aus.
START DUMP
Hauptmenü
Abbrechen


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
msm-net VPN/Firewall-Rout...
https://192.1...vice_tcpdump
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
11:26:17.546332 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) 192.168.32.240 > 192.168.32.254: ICMP echo request, ic
11:26:17.546442 IP (tos 0x0, ttl 64, id 26075, offset 0, flags [none], proto: ICMP (1), length: 84) 192.168.32.254 > 192.168.32.240: ICMP echo reply
11:26:18.546179 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) 192.168.32.240 > 192.168.32.254: ICMP echo request, ic
11:26:18.546315 IP (tos 0x0, ttl 64, id 26076, offset 0, flags [none], proto: ICMP (1), length: 84) 192.168.32.254 > 192.168.32.240: ICMP echo reply
11:26:19.546024 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) 192.168.32.240 > 192.168.32.254: ICMP echo request, ic
5 packets captured
6 packets received by filter
0 packets dropped by kernel

HINWEIS	
	Das Ergebnis des „Netzwerk Dumps“ wird erst nach dem vollständigen Durchlaufen des Befehls angezeigt. Eine kleinere Anzahl von Pakete führt daher rascher zum Ergebnis. Wenn keine Pakete mit den angegebenen Parametern gesendeten oder empfangenen werden, wird auch kein Ergebnis angezeigt. Ergebnisfenster oder Tabs können einfach geschlossen werden.

„Traceroute“:

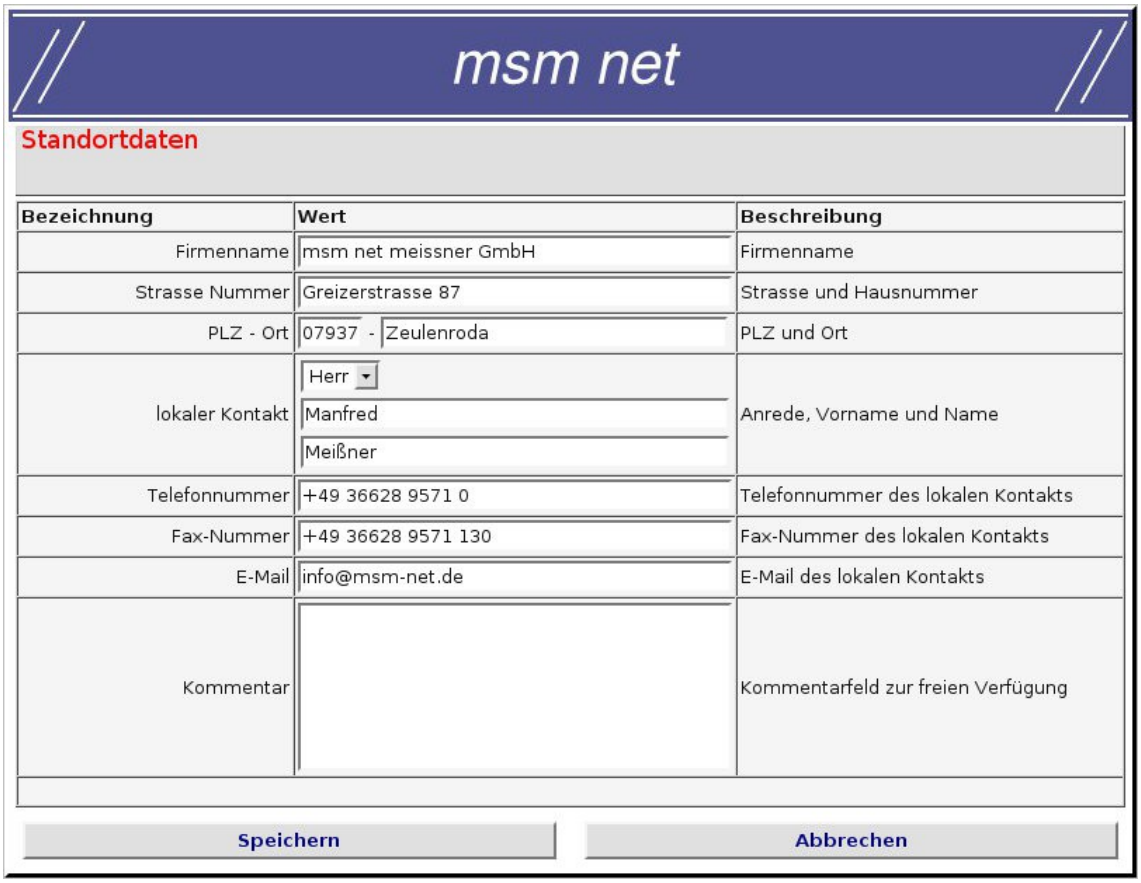


NOTE	
	Das Ergebnis des „Traceroute“ wird erst nach dem vollständigen Durchlaufen des Befehls angezeigt. Eine kleinere Anzahl von abzufragenden HOPS führt daher rascher zum Ergebnis. Ergebnisfenster oder Tabs können einfach geschlossen werden.

6.8. Standortdaten

In den Standortdaten können Kontaktdaten eines Vor-Ort-Ansprechpartners eingetragen werden. Dies hat sich insbesonders bei größeren Installationen bewährt.

Das Menü „Standortdaten“ der VPN Appliance:



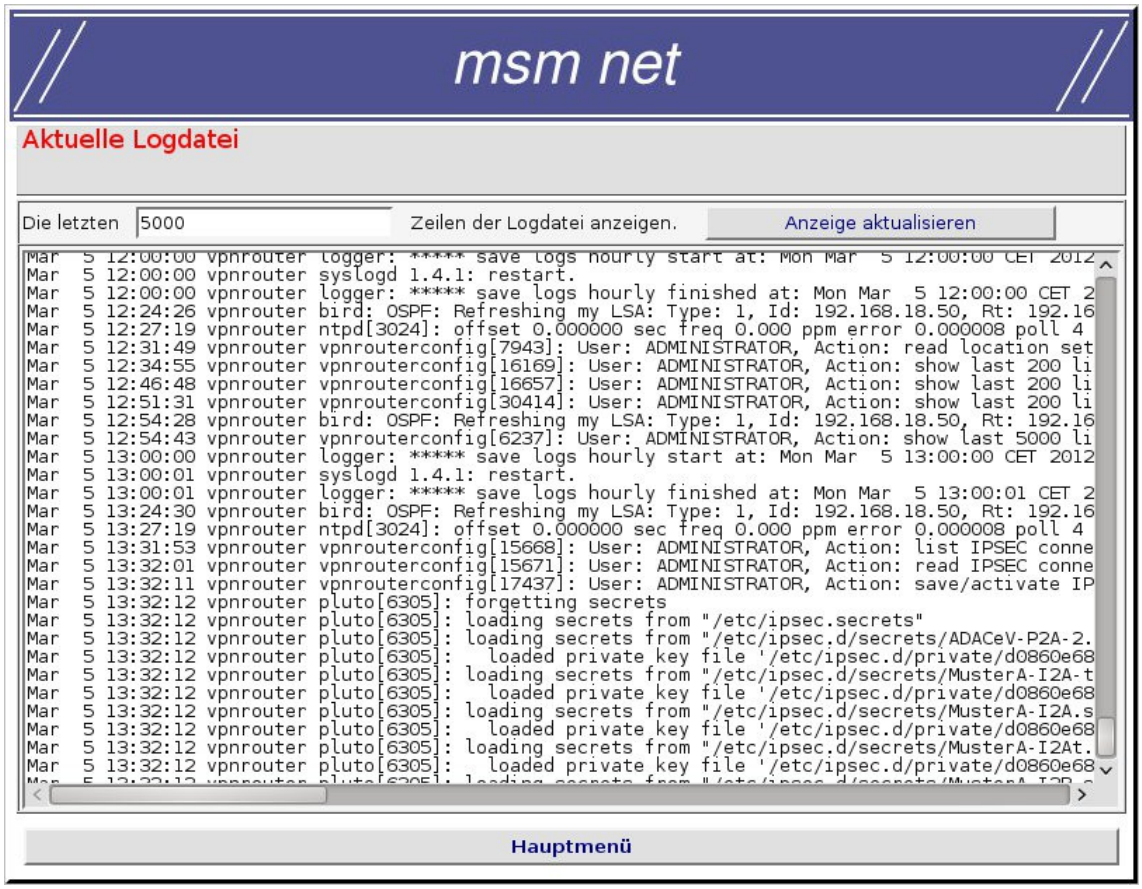
6.9. Logdatei

Mithilfe des Menüpunktes „Aktuelle Logdatei einsehen“ ist es möglich, die aktuelle Logdatei der VPN Appliance direkt einzusehen. In der Standardkonfiguration werden beispielsweise allgemeine Informationen über den Systemzustand, die VPN Verbindungen, die Authentifizierung, der Administration und Firewall Ereignisse protokolliert. Alle 24 Stunden wird ein Spool-Vorgang zum Archivieren der Logdatei gestartet.

Der Versand der Logdatei per E-Mail, kann in dem Menü „Allgemeine Einstellungen“ konfiguriert werden.

Darüber hinaus bietet die msm net meissner GmbH einen zentralen Log-Server für das Management der Log-Dateien an.

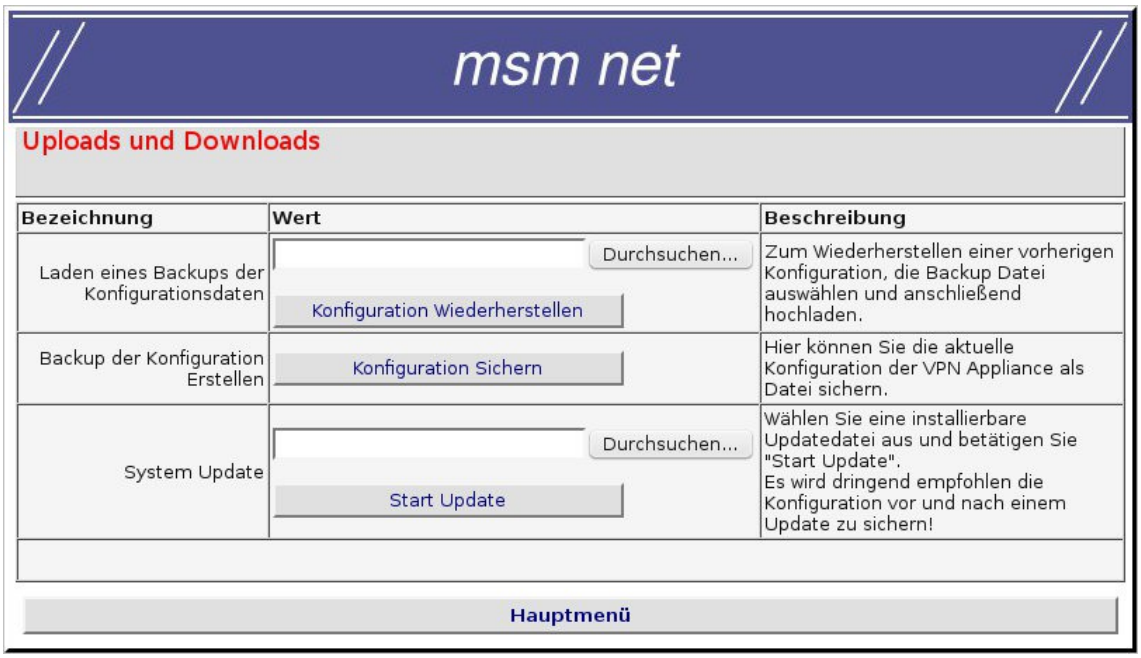
Das Menü „Aktuelle Logdatei einsehen“:


msm net
Aktuelle Logdatei
Die letzten 5000 Zeilen der Logdatei anzeigen.
Anzeige aktualisieren
Mar 5 12:00:00 vpnrouter logger: ***** save logs hourly start at: Mon Mar 5 12:00:00 CET 2012
Mar 5 12:00:00 vpnrouter syslogd 1.4.1: restart.
Mar 5 12:00:00 vpnrouter logger: ***** save logs hourly finished at: Mon Mar 5 12:00:00 CET 2
Mar 5 12:24:26 vpnrouter bird: OSPF: Refreshing my LSA: Type: 1, Id: 192.168.18.50, Rt: 192.16
Mar 5 12:27:19 vpnrouter ntpd[3024]: offset 0.000000 sec freq 0.000 ppm error 0.000008 poll 4
Mar 5 12:31:49 vpnrouter vpnrouterconfig[7943]: User: ADMINISTRATOR, Action: read location set
Mar 5 12:34:55 vpnrouter vpnrouterconfig[16169]: User: ADMINISTRATOR, Action: show last 200 li
Mar 5 12:46:48 vpnrouter vpnrouterconfig[16657]: User: ADMINISTRATOR, Action: show last 200 li
Mar 5 12:51:31 vpnrouter vpnrouterconfig[30414]: User: ADMINISTRATOR, Action: show last 200 li
Mar 5 12:54:28 vpnrouter bird: OSPF: Refreshing my LSA: Type: 1, Id: 192.168.18.50, Rt: 192.16
Mar 5 12:54:43 vpnrouter vpnrouterconfig[6237]: User: ADMINISTRATOR, Action: show last 5000 li
Mar 5 13:00:00 vpnrouter logger: ***** save logs hourly start at: Mon Mar 5 13:00:00 CET 2012
Mar 5 13:00:01 vpnrouter syslogd 1.4.1: restart.
Mar 5 13:00:01 vpnrouter logger: ***** save logs hourly finished at: Mon Mar 5 13:00:01 CET 2
Mar 5 13:24:30 vpnrouter bird: OSPF: Refreshing my LSA: Type: 1, Id: 192.168.18.50, Rt: 192.16
Mar 5 13:27:19 vpnrouter ntpd[3024]: offset 0.000000 sec freq 0.000 ppm error 0.000008 poll 4
Mar 5 13:31:53 vpnrouter vpnrouterconfig[15668]: User: ADMINISTRATOR, Action: list IPSEC conne
Mar 5 13:32:01 vpnrouter vpnrouterconfig[15671]: User: ADMINISTRATOR, Action: read IPSEC conne
Mar 5 13:32:11 vpnrouter vpnrouterconfig[17437]: User: ADMINISTRATOR, Action: save/activate IP
Mar 5 13:32:12 vpnrouter pluto[6305]: forgetting secrets
Mar 5 13:32:12 vpnrouter pluto[6305]: loading secrets from "/etc/ipsec.secrets"
Mar 5 13:32:12 vpnrouter pluto[6305]: loading secrets from "/etc/ipsec.d/secrets/ADACeV-P2A-2.
Mar 5 13:32:12 vpnrouter pluto[6305]: loaded private key file '/etc/ipsec.d/private/d0860e68
Mar 5 13:32:12 vpnrouter pluto[6305]: loading secrets from "/etc/ipsec.d/secrets/MusterA-I2A-t
Mar 5 13:32:12 vpnrouter pluto[6305]: loaded private key file '/etc/ipsec.d/private/d0860e68
Mar 5 13:32:12 vpnrouter pluto[6305]: loading secrets from "/etc/ipsec.d/secrets/MusterA-I2A.s
Mar 5 13:32:12 vpnrouter pluto[6305]: loaded private key file '/etc/ipsec.d/private/d0860e68
Mar 5 13:32:12 vpnrouter pluto[6305]: loading secrets from "/etc/ipsec.d/secrets/MusterA-I2At.
Mar 5 13:32:12 vpnrouter pluto[6305]: loaded private key file '/etc/ipsec.d/private/d0860e68
Hauptmenü

6.10. Upload und Download

Über das Menü „Upload / Download“ wird eine Funktion für Backup und Wiederherstellung der Systemeinstellungen auf bzw. von einem lokalen Administrationshost zur Verfügung gestellt. Außerdem wird in diesem Menü die Update-Funktion zur Verfügung gestellt. Der Update-Prozess setzt jedoch ein gültiges Update voraus.

Das Menü „ Upload / Download“:


msm net
Uploads und Downloads
Bezeichnung
Wert
Beschreibung
Laden eines Backups der Konfigurationsdaten
Durchsuchen...
Konfiguration Wiederherstellen
Zum Wiederherstellen einer vorherigen Konfiguration, die Backup Datei auswählen und anschließend hochladen.
Backup der Konfiguration Erstellen
Konfiguration Sichern
Hier können Sie die aktuelle Konfiguration der VPN Appliance als Datei sichern.
System Update
Durchsuchen...
Start Update
Wählen Sie eine installierbare Updatedatei aus und betätigen Sie "Start Update".
Es wird dringend empfohlen die Konfiguration vor und nach einem Update zu sichern!
Hauptmenü

NOTE	
	Es wird dringend empfohlen, vor und nach dem Einspielen eines Updates, die aktuellen Konfigurationsdaten zu sichern!

7. Service und Wartung

Die msm net meissner GmbH bietet allen Kunden umfassende Beratungs-, Wartungs- und Serviceleistungen für die Projektierung, die Realisierung und den Betrieb einer VPN Lösung an.

Orientiert an der eigenen Leistungsfähigkeit und den spezifischen Anforderungen des Kunden, können individuelle SLAs definiert und in Wartungs- und Serviceverträgen umgesetzt werden.

Je nach Größe der zu betreibenden VPN Installation und den betriebsbedingten Anforderungen eines Kunden, können optional, zentrale Managementstrukturen mittels eines Managementservers sowie eines zentralen Log-Servers realisiert werden.

Begleitend zu den eher technischen Maßnahmen bietet msm net verschiedenste Servicezeiten (z.B. 10x5, 24x7, ...) an. Somit können wir den vielfältigsten kundenspezifischen Anforderungen gerecht werden.

8. Technische Daten

8.1. Bauformen

Die VPN Appliances der msm net meissner GmbH können mit allen am Markt zur Verfügung stehenden Standardgehäusen realisiert werden. Dies bedeutet hinsichtlich der Bauformen, das die Lieferung in folgenden Gehäusen möglich ist:

Gehäuseauswahl	
Custom – Gehäuse	
19 -Zoll 1HE – Gehäuse	
19 -Zoll 2HE – Gehäuse	
Server – Gehäuse	

Die Gehäuseauswahl ist nur insofern frei, wie es die technischen Gegebenheiten und Anforderungen an das System zulassen. Sie wird insbesondere von der Ausstattung mit Schnittstellen und der Leistungsklasse bestimmt. Eine größere Leistungsklasse stellt auch höhere Anforderungen hinsichtlich Energieverbrauch und Kühlbedarf.

Leistungsstufen	**Daten Durchsatz**
Mini	< 1 Mbyte/sec
Midi	< 10 Mbyte/sec
Maxi	> 80 Mbyte/sec

8.2. Leistungsparameter der VPN Appliance

Kategorie	Details
Betriebssystem	Linux
Hardware Systemplattform	Industrie PC-Komponenten, Server-Komponenten, Skalierbar nach projektbezogenen Anforderungen
Anzahl der möglichen VPN Verbindungen	Nur durch die eingesetzte Hardware begrenzt.
Datendurchsatz	Begrenzt durch die verwendete Methode Begrenzt durch die Leistungsstufe
Authentifizierungsverfahren	MD5 SHA1 SHA2-256 SHA2-384 SHA2-512
Verschlüsselungsalgorithmen	3DES 192 AES 128 / 192 / 256 Blowfish 128 / 192 / 256 CAST6 128 / 192 / 256 Twofish 128 / 192 / 256 Serpent 128 / 192 / 256
Bitlängen der DH MODP Group	786 1024 1536 2048 3072 4096 6144 8192
VPN Verbindungsmethoden	IPSEC PPTP L2TP
IP Adressschema	IPv4 und IPv6 (intern) statisch und dynamisch
Automatische Verbindungstrennung	konfigurierbar

Kategorie	Details
Automatische Schlüsselaktualisierung	konfigurierbar
Zertifikat Verwaltung	Root-CA- oder Sub-CA-Zertifikate Authentifizierungs-Zertifikate CRL und OCSP Cryptosmartcard-Applikation
Authentifizierung	X.509 Zertifikate konfigurierbar mit/ohne CRL und / oder OSCP Pre-Shared Key
Logdatenmanagement	Konfigurierbar Versand per E-Mail Versand per Syslog
Systemredundanz	Redundanz Steuerung für die Nutzung des Übertragungsmediums und Verfügbarkeit der VPN Appliances

8.3. Basis RFC der VPN Software

Allgemeine RFCs / Overview RFCs

2401 Security Architecture for the Internet Protocol

2411 IP Security Document Roadmap

Basis Protokolle / Basic Protocols

2402 IP Authentication Header

2406 IP Encapsulation Security Payload (ESP)

Schlüssel Verwaltung / Key Management

2367 PF_KEY Key Management API, Version 2

2407 The Internet IP Security Domain of Interpretation for ISAKMP

2408 Internet Security Association and Key Management Protocol (ISAKMP)

2409 The Internet Key Exchange (IKE)

2412 The OAKLEY Key Determination Protocol

2528 Internet X.509 Public Key Infrastructure

Details zu einzelnen genutzten Dingen / Details of various things used

2085 HMAC-MD5 IP Authentication with Replay Prevention

2104 HMAC: Keyed-Hashing for Message Authentication

2202 Test Cases for HMAC-MD5 and HMAC-SHA-1

2207 RSVP Extensions for IPSEC Data Flows

2403 The Use of HMAC-MD5-96 within ESP and AH

2404 The Use of HMAC-SHA-1-96 within ESP and AH

2405 The ESP DES-CBC Cipher Algorithm With Explicit IV

2410 The NULL Encryption Algorithm and Its Use With IPSEC

2451 The ESP CBC-Mode Cipher Algorithms

2521 ICMP Security Failures Messages

Ältere RFC die referenziert sein können / Older RFCs which may be referenced

1321 The MD5 Message-Digest Algorithm

1828 IP Authentication using Keyed MD5

1829 The ESP DES-CBC Transform

1851 The ESP Triple DES Transform

1852 IP Authentication using Keyed SHA

Mitgeltende RFCs / Related RFCs

1750 Randomness Recommendations for Security

1918 Address Allocation for Private Internets

1984 IAB and IESG Statement on Cryptographic Technology and the Internet

2144 The CAST-128 Encryption Algorithm

9. Entsorgungshinweise

Informationen zur Sammlung und Entsorgung von gebrauchten elektrischen oder elektronischen Geräten.

Bitte führen Sie dieses Produkt nach seiner Verwendung entsprechend den aktuellen EU-Entsorgungsvorschriften als Elektronikschrott einer geordneten Entsorgung zu.

Sollte dies in Ihrem Umfeld nicht möglich sein, übernehmen wir für Sie die Entsorgung.